FSD J1708 Product Family User Manual

View Installation Guide

View Configuration Guide

View Reference Manuals

View Product Specifications

FSD J1708 Installation Guides

Select the FSD J1708 application below to display its configuration manual.

FSD J1708 Tester Installation Guide - FSD J1708/J1587 Tester allows developers to debug software and hardware developed for use with J1708 communication protocol.

FSD J1708 Bridge Installation Guide - FSD J1708/J1587 Bridge allows access of data from one data bus to another data bus.

FSD J1708 Logger Installation Guide - FSD J1708/J1587 captures data packets transmitted across the J1708 data busses.

FSD J1708 Tester Installation Guide

For the FSD J1708 Tester:

1. Unpack the shipping box. It should contain:

a. FSD J1708 Tester Controller (labeled FSD Compact Controller)

b. Installation disk

c. USB cable

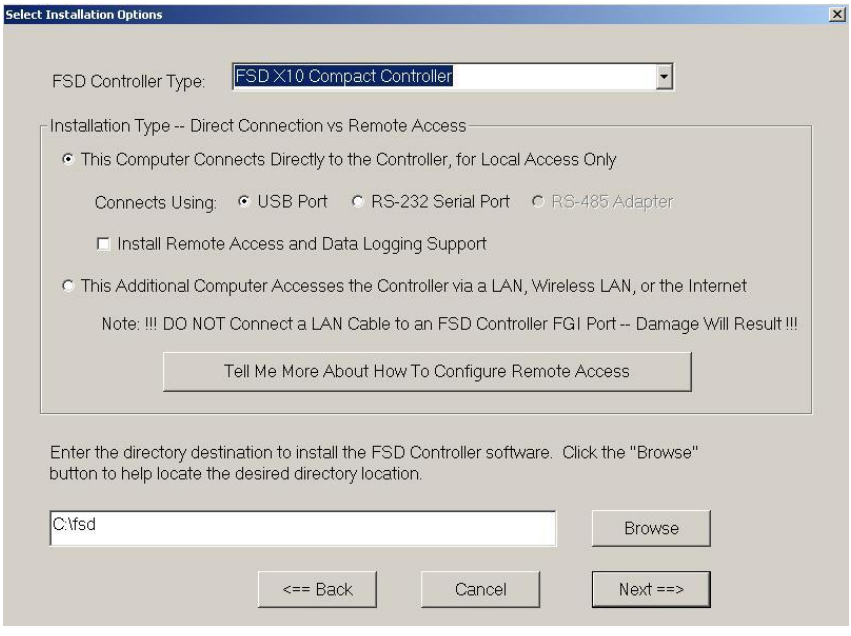
d. Power transformer, 9 VAC

DO NOT plug any cables into the FSD Compact Controller at this time.

2. Install programs

a. Insert the Installation CD into the CD or DVD drive of your computer.

b. The installer starts automatically. If not, open Windows Explorer and select the CD or DVD drive. Double-click on \fsd\bin\install_j1708_tester application to start installing files.


Select Installation Options
FSD Controller Type:
FSD X10 Compact Controller
Installation Type -- Direct Connection vs Remote Access
This Computer Connects Directly to the Controller, for Local Access Only
Connects Using:
USB Port
RS-232 Serial Port
RS-485 Adapter
Install Remote Access and Data Logging Support
This Additional Computer Accesses the Controller via a LAN, Wireless LAN, or the Internet
Note: !!! DO NOT Connect a LAN Cable to an FSD Controller FGI Port -- Damage Will Result !!!
Tell Me More About How To Configure Remote Access
Enter the directory destination to install the FSD Controller software. Click the "Browse" button to help locate the desired directory location.
C:\fsd
Browse
<== Back
Cancel
Next ==>

c. Click the “Install Software” button to begin installation.

d. Read the License Agreement, and click the “I agree” button to continue. Use the “<–Back” and “Next” buttons to navigate within the installer.

f. For the initial installation, select the J1708 Tester (controller attached to computer) controller type, and set the type of connection port to USB Port.

g. Alternatively, if setting up an additional computer, select the (controller accessed via Internet or LAN) installation type, and read the remote access configuration instructions.

h. Enter the installation root directory destination in the edit box or choose the directory with the “Browse” button. We suggest the default setting.

i. Verify selected options before proceeding to install.

3. Connect the Controller:

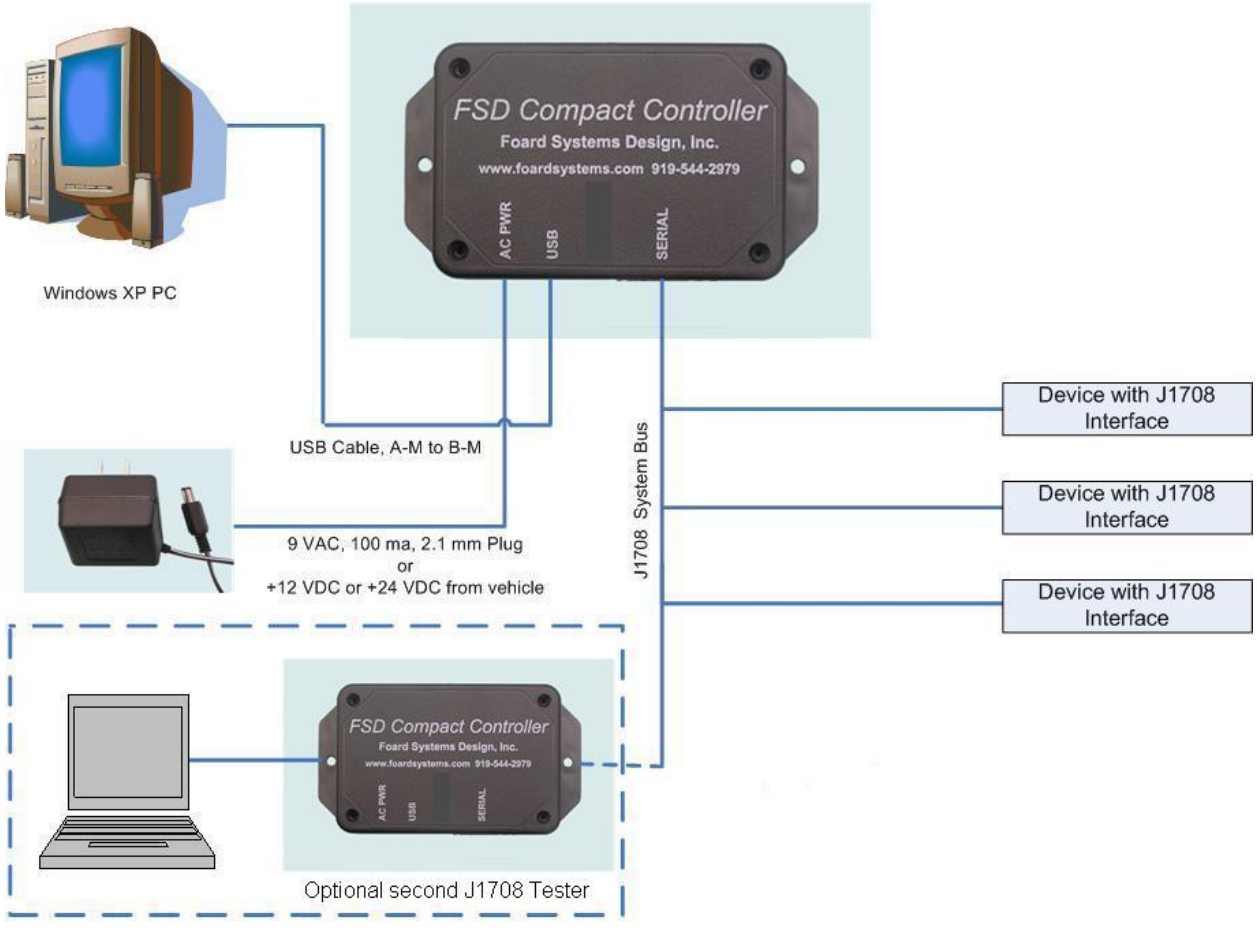
After the software installation succeeds, connect the controller cables as shown in the picture at the end of this section.

a. Plug the power transformer into an electrical receptacle and insert into the controller box at the port marked “AC PWR”.

b. Connect the USB cable to the USB port on your computer and the other end to the port marked “USB” on the FSD Compact Controller box. Windows XP should find and recognize the new device.

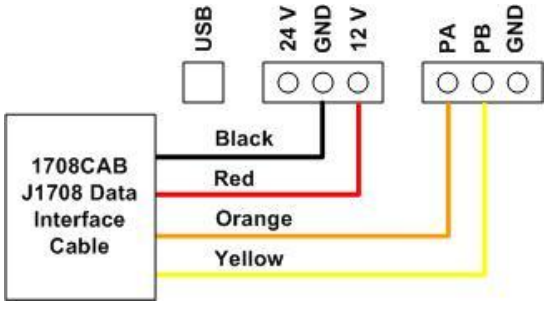
4. Operation

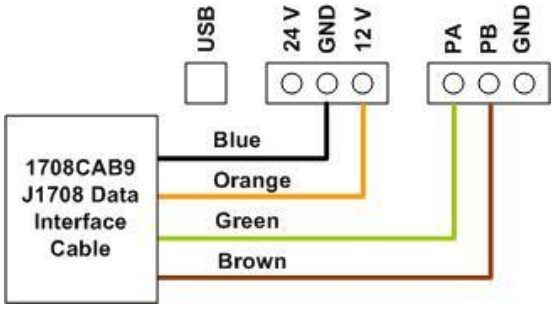
For normal operation, start the software by running Autostart from the “bin” folder in the directory you specified during installation. Autostart setting options are found in the J1708 Tester Options menu, by selecting “Set Autostart Options”.



J1708 Tester Installation

The following diagrams illustrate how to connect J1708 data bus systems to the FSD J1708 Tester. The cables illustrated are from B & B Electronics Mfg. Co., 707 Dayton Rd. Ottawa, Ill 61350. The colored wire corresponds to Model 1708CAB, left diagram, and Model 1708CAB9, right diagram.





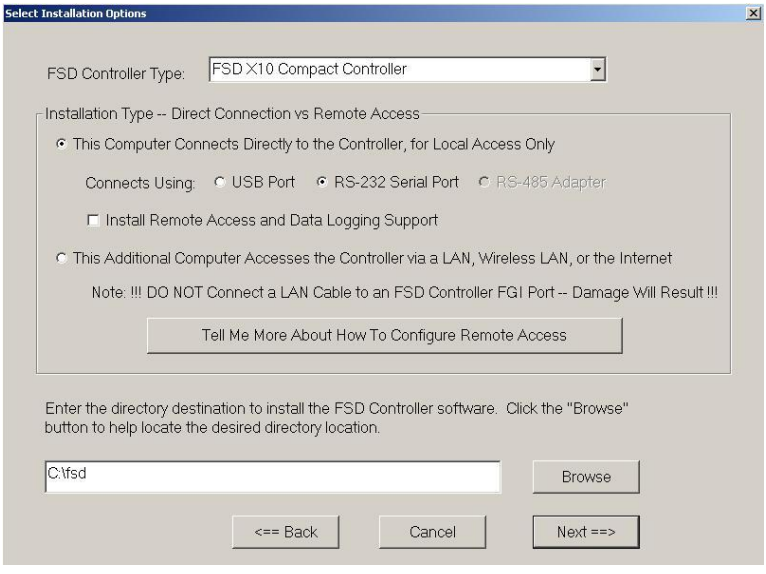
FSD J1708 Bridge and FSD J1708 Logger Installation Guide

For the FSD J1708 Bridge or FSD J1708 Logger:

1. Unpack the shipping box. It should contain:

a. FSD 1708 Bridge or Logger Controller (FSD Compact Bridge)

b. Installation disk


Select Installation Options
FSD Controller Type:
FSD X10 Compact Controller
Installation Type -- Direct Connection vs Remote Access
This Computer Connects Directly to the Controller, for Local Access Only
Connects Using:
USB Port
RS-232 Serial Port
RS-485 Adapter
Install Remote Access and Data Logging Support
This Additional Computer Accesses the Controller via a LAN, Wireless LAN, or the Internet
Note: !!! DO NOT Connect a LAN Cable to an FSD Controller FGI Port -- Damage Will Result !!!
Tell Me More About How To Configure Remote Access
Enter the directory destination to install the FSD Controller software. Click the "Browse" button to help locate the desired directory location.
C:\fsd
Browse
<== Back
Cancel
Next ==>

2. Install programs

a. Insert the Installation CD into the CD or DVD drive of your computer.

b. The installer starts automatically. If not, open Windows Explorer and select the CD or DVD drive. Double-click on \fsd\bin\install_j1708_bridge application to start installing files.

c. Click the “Install Software” button to begin installation.

d. Read the License Agreement, and click the “I agree” button to continue. Use the “<–Back” and “Next” buttons to navigate within the installer.

f. For the initial installation, select the (controller attached to computer) installation type, and set the type of connection port to USB Port.

g. Alternatively, if setting up an additional computer, select the (controller accessed via Internet or LAN) installation type, and read the remote access configuration instructions.

h. Enter the installation root directory destination in the edit box or choose the directory with the “Browse” button.

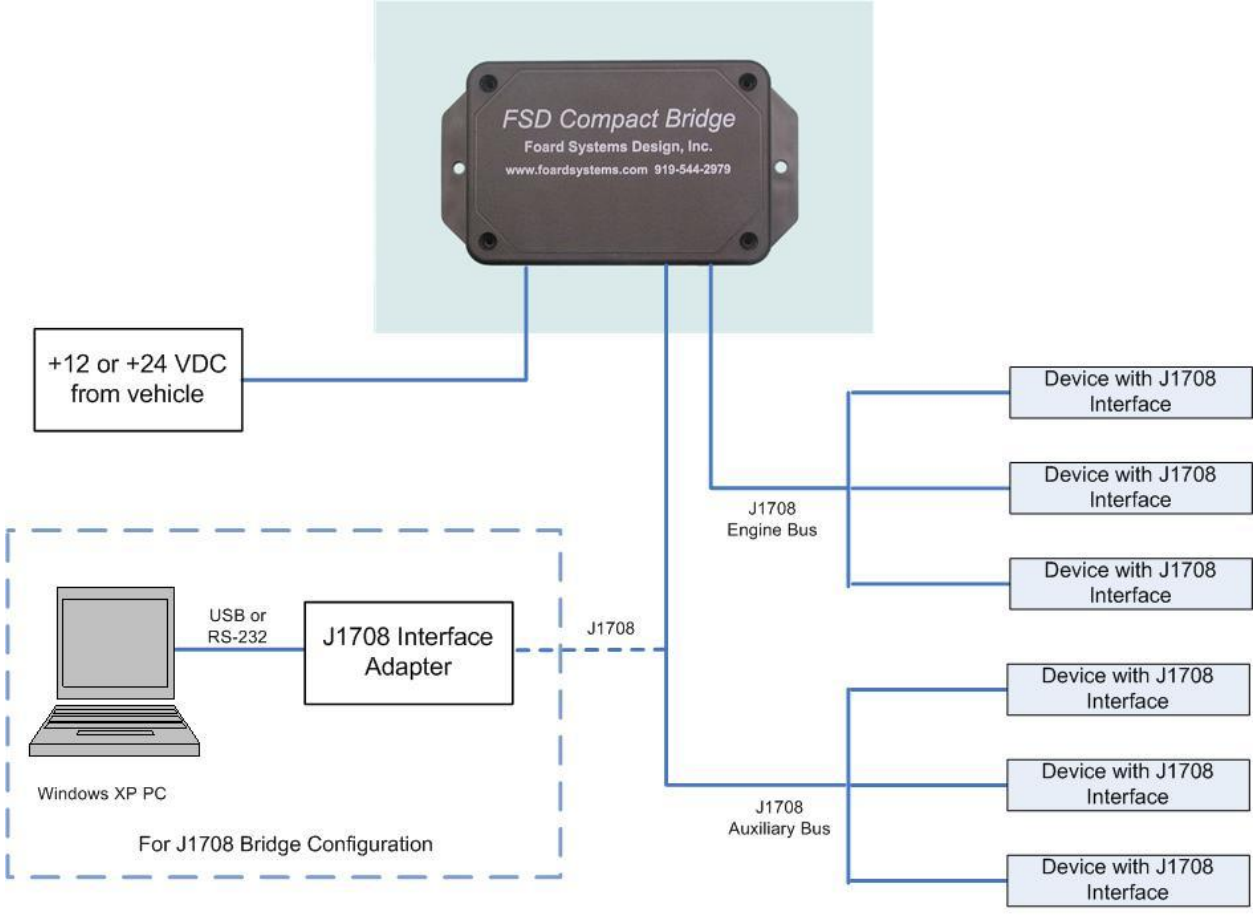
i. Verify selected options before proceeding to install.

3. Connect the Controller:

After the software installation succeeds, connect the controller wires as shown in the picture at the end of this section.

a. At the JP8 header connect the power (either 12V or 24V) supply wire and ground wire.

b. Attach the appropriate wires from your device to the serial screw-in port, as indicated on page 3.

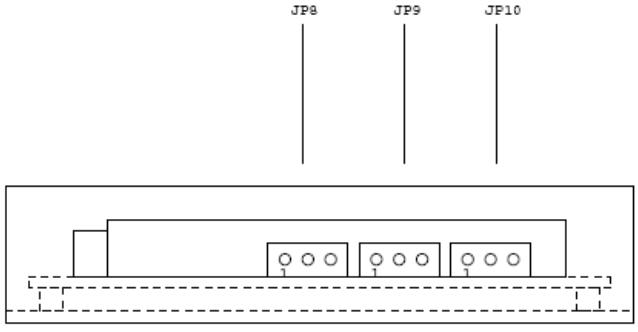


FSD J1708 Bridge Installation

4. Operation

For normal operation, start the software by running Autostart from the "bin" folder in the directory you specified during installation. Autostart setting options are found in the J1708 Bridge Options menu, by selecting "Set Autostart Options".

J1708 Bridge



JP8 Power Input
- 1) 24V Input
- 2) GND Input
- 3) 12V Input (If 24V not used)

JP9 J1708 Interface
- 1) SA J1708 +
- 2) SB J1708 -
- 3) J1708 GND

JP10 RS232 Interface
- 1) FSD J1708 Bridge RS232 TXD
- 2) FSD J1708 Bridge RS232 RXD
- 3) GND

FSD J1708 Configuration Guides

Select the FSD J1708 application or topic below to display its configuration manual.

FSD J1708 Tester Operation Guide - Configuration manual for J1708 Tester.

FSD J1708 Bridge Operation Guide - Configuration manual for J1708 Bridge.

FSD J1708 Logger Operation Guide – Configuration manual for J1708 Logger.

FSD J1708 Control Software Operation Guide

FSD J1708/J1587 Control is a utility used to configure the operation of the FSD J1708 Bridge and FSD J1708 Logger. FSD J1708 Control is typically access via a submenu item in the J1708 Bridge or J1708 Logger application, but may be run as a stand-alone application.

FSD J1708 Tester Operation Guide

Run Time Monitoring:

The FSD J1708 Tester software, in the default configuration, displays received J1708 packet data in decimal format, and also shows decoded packet information. Figure 1 shows a typical monitored J1708 session.

In the screen shown, the arrow symbol preceeding the decimal J1708 packet line shows the packet direction. Rightward arrows indicate packets originated by the FSD J1708 Tester and leftward arrows indicate other packets received from the J1708 bus. A hex representation of the packet transmission date/time also preceeds the J1708 packet data.

The semicolon preceeding the decoded data denotes the line as a "comment line". The same annotation style is used in FSD's simulation script files.

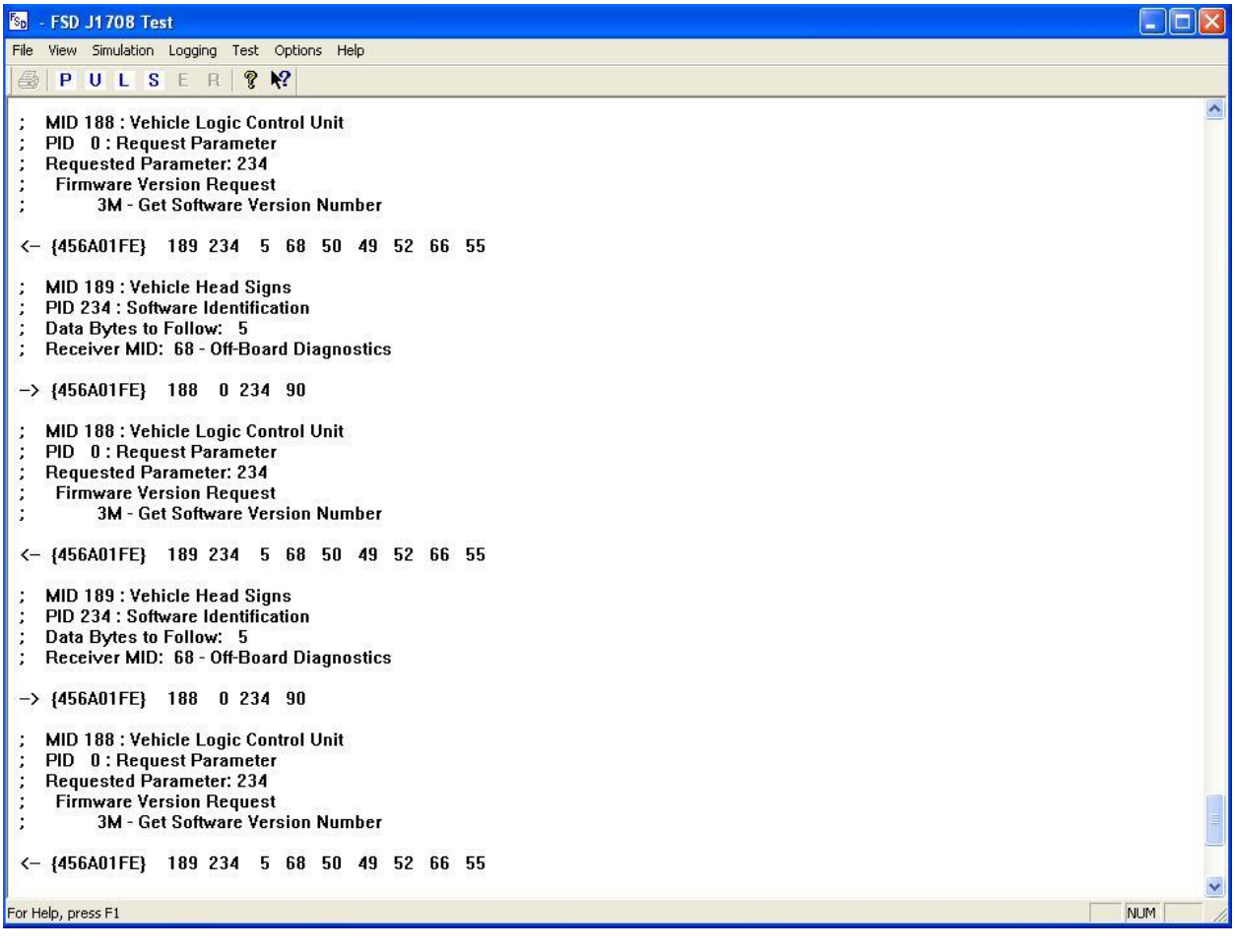


Figure 1: FSD J1708 Tester

Data Logging:

Monitored J1708 packets can be saved to a log file, either as a space efficient binary file or as a text file with similar contents as the monitoring screen. Figure 2 shows the Logging options on the J1708 Tester main menu.

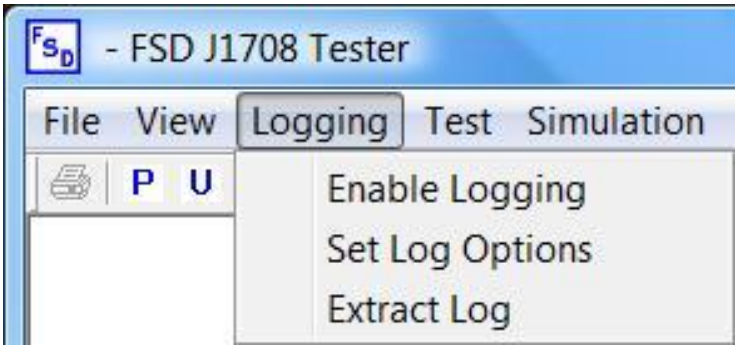


Figure 2: FSD J1708 Tester

From the Logging menu choose Set Log Options to configure logging parameters.

Figure 3 shows the Log Options dialog used to configure logging options. Enter (1) the path to the directory to save the log file, (2) whether logging is selected as a default setting and (3) whether to save as a text or binary file. In the middle section, select whether to show packets only (no decoding), decode all packets, decode packets with specific MIDs, or decode packets with the exception of the listed MIDs.

If one chooses to decode all packets partially, just the MID and PID information is shown per packet.

(The ability to log to flash memory is not standard on FSD J1708 Tester, but can be part of the FSD J1708 Bridge with Logger features.)

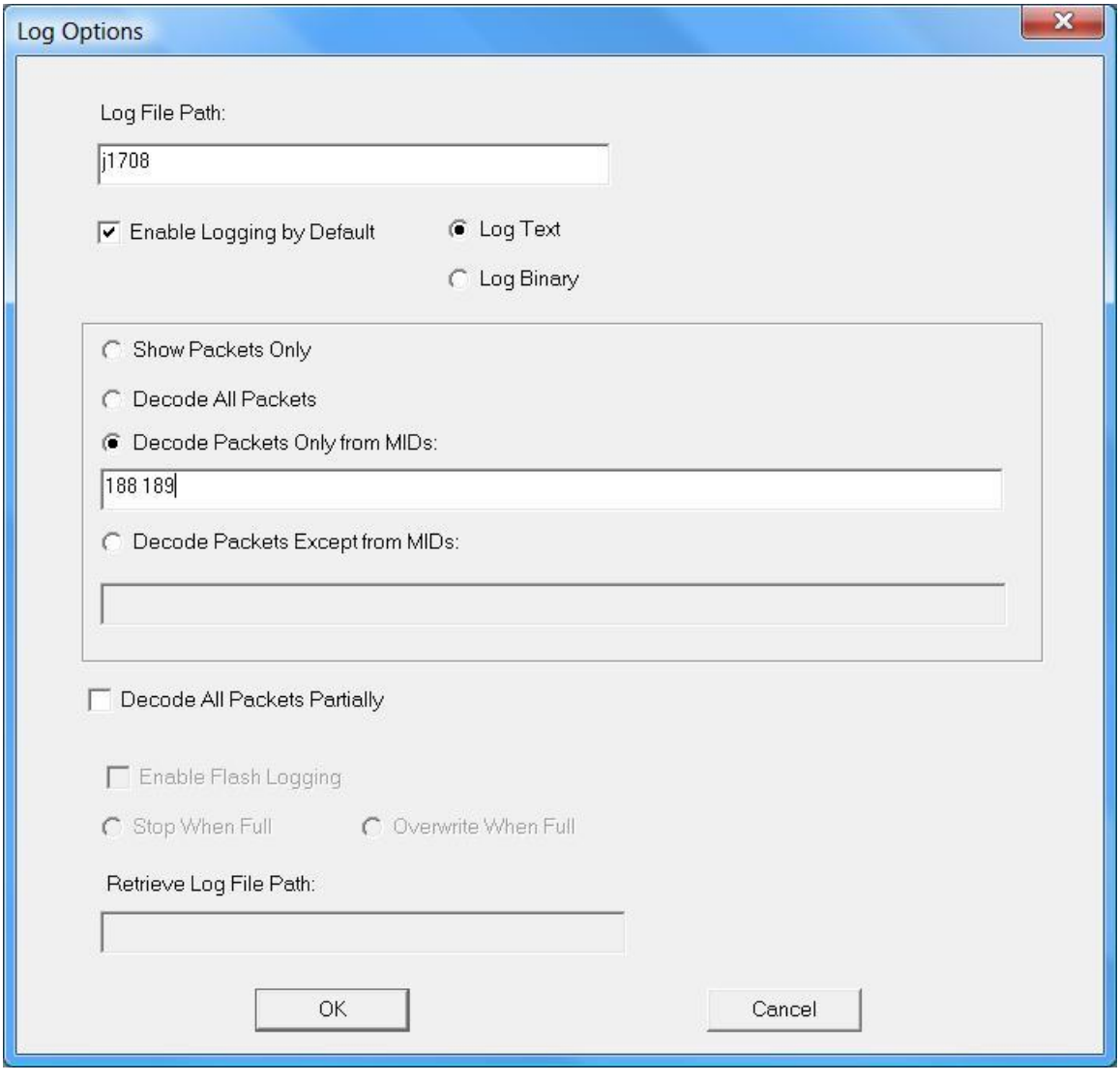


Figure 3: Set Log Options

If saved as a binary file, use the "Extract Log" option to convert the binary file into a text file, with packet decoding as an option. The following dialog is displayed (Fig 4). Choose the binary file saved from the droplist. (The files are in the data directory of your install directory with filetype "jt_blog".) Select whether you want only packets shown or packets decoded. By indicating the specific MIDs, these MIDs can either be the only packets decoded, or the packets not decoded. If you check Decode All Packets Partially, each packet will have its MID and PID(s) displayed, without any data decoded.

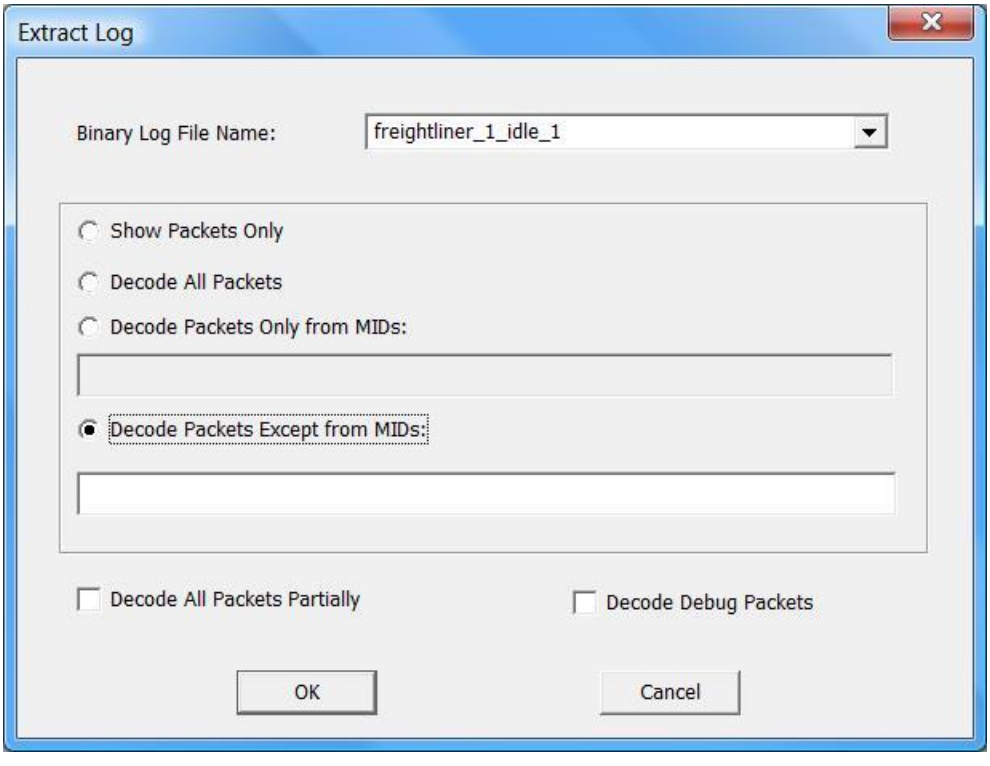


Figure 4: Extract Log Options

Sending Test Packets:

For testing device response to individual packet types, the FSD J1708 Tester can send both properly formed and improperly formed packets with arbitrary content. Figure 5 shows the individual packet tests available under the Test menu. Use the "Predefined Packets" option for customized testing of a specific device, as discussed in the "Customization Options" section (see below). Use the "User Defined Packets" option to send arbitrarily defined packets, using the "Send User Defined Packets" dialog box shown in Figure 6.

If checked. the system calculates the packet checksums, which simplifies packet construction However, you need to enter a placeholder number (e.g. "0") at the end of the packet. The program replaces this number with the checksum. Disable the feature to test the device's response to packets with incorrect checksums.

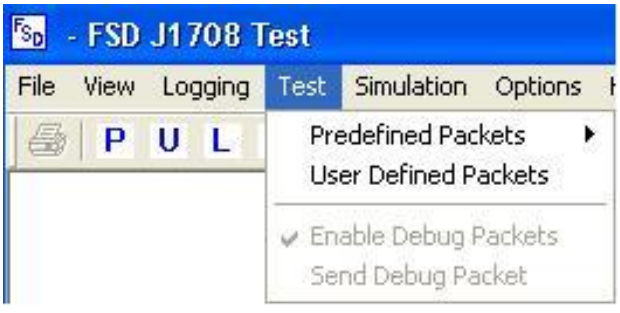


Figure 5: Test Menu Options

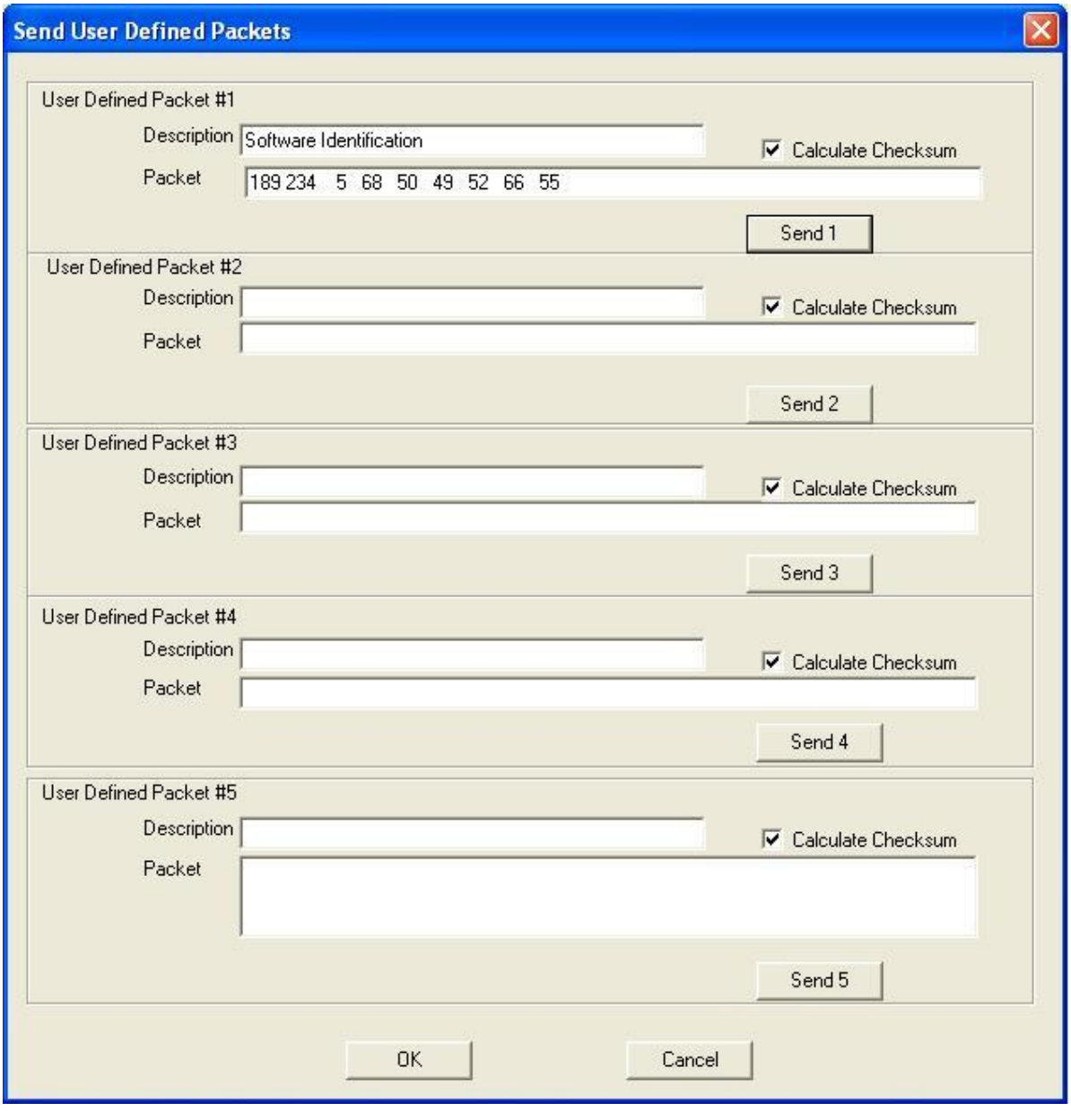


Figure 6: User Defined Packets

Simulation:

The FSD J1708 Tester offers two simulation methods -- script and scenario. Figure 7 shows the menu options for configuring and running simulation scripts and scenarios.

The script file method is a simple, extremely easy-to-use approach to debug most J1708 problems. One can generate a script file by using the Logging option to capture a test session containing the problem to debug. Simply rename the log file as a simulation file for replay (replace jt_blog extension with jt_scr. Alternatively, if a problem arises while monitoring and not logging, one can cut and past the monitored session from the Tester screen into a file using any editor that supports Paste, such as Notepad, Word, or a programming editor. A script file (jt_scr extension) made from either approach can be used either without modification, or with editing to add or remove packets and/or add comments, as desired.

The scenario method allows the user to delineate and run a collection of user defined scenarios. Each scenario can be constructed as a time-varying combination of repetitive packets and arbitrary script defined sequences.

Script and scenario methods can be used simultaneously with their packets interleaved. Use either method to stress test a system over a long time period by setting the simulation options to repeat the script or scenario continuously, and logging the monitored session to a data file.

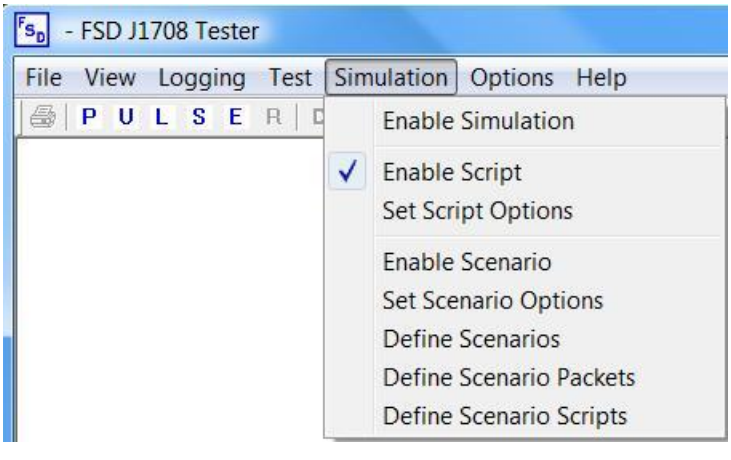


Figure 7: Simulation Menu Options

<u>Simulation Scripts:</u>

To configure a simulation script, from the Simulation menu choose Set Script Options. The Script Options dialog is displayed (Figure 8). Select "Use Source Timing" option to base the transmitted packet timing on the packet timing recorded in the simulation script file (relative to the first packet listed). One can edit the source timing by applying minimum and maximum time limits or use randomized timing, which adds or subtracts an amount (limited range) to the source time.

Otherwise, the time betweens packets is randomized between the specified minimum and maximum time limits.

All packets in the script or only all transmitted (TX) packets may be sent. The "Send TX Packets Only" mode simplifies reuse of a captured log file as a simulation script, by filtering out response packets from other devices on the J1708 bus and only resending the packets that were originally sent from the J1708 Tester. Alternatively, a set of device MIDs can be specified, with the script sending either the packets matching the listed MIDs or all packets excluding the listed MIDs.

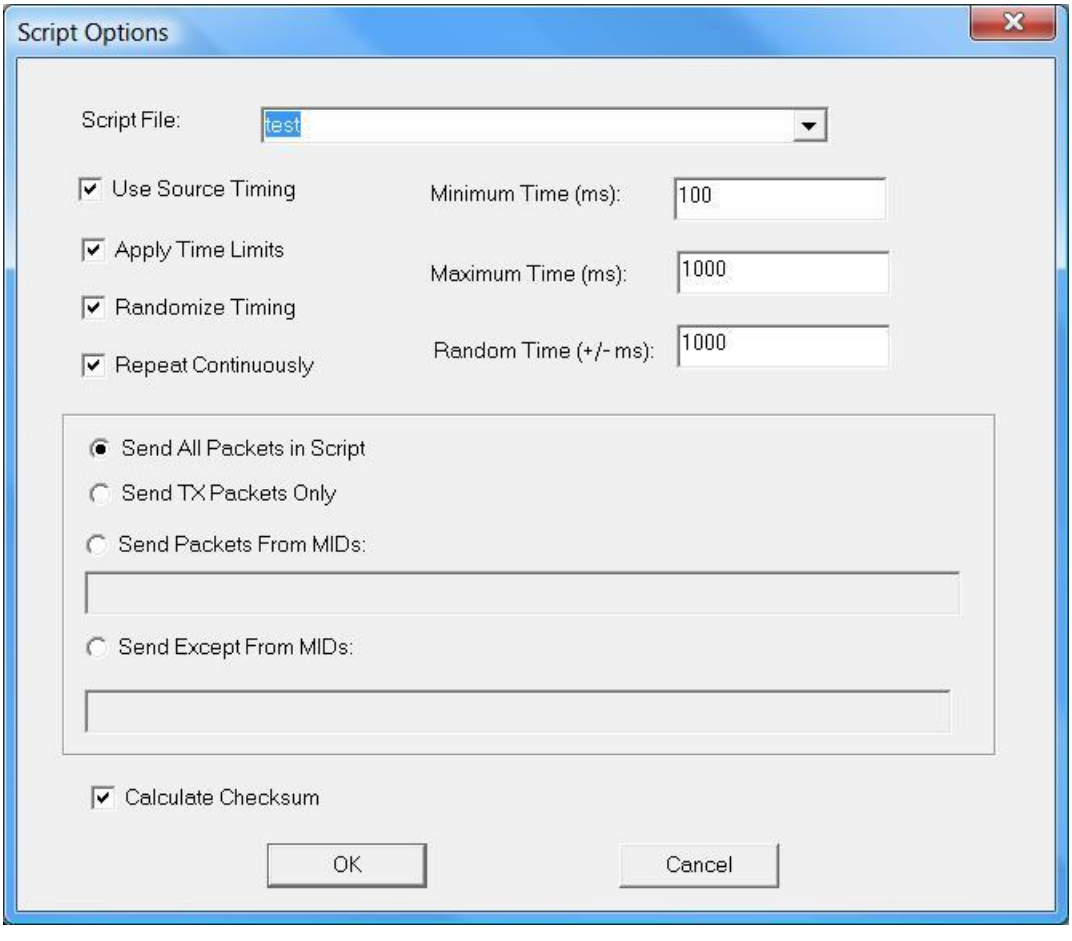


Figure 8: Simulation Script Options

Simulation Scenarios:

Scenarios are constructed by first specifying a sequence of time frames, and second detailing a set of repetitive packets and / or a set of scripts to run during the time frames. The suggested approach to configure a scenario is to define the repetitive packets and scripts, followed by assembling them into the desired time frames. One can configure multiple scenario definitions and select each singly for use.

Packet sets collect packets. Scenarios use packets from within a selected packet set. Different scenarios can use the same packet sets. Figure 9 shows the packet definition approach. To configure a simulation script, from the Simulation menu choose Define Scenario Packets. Use the Edit Scenario Packet Sets dialog to select or insert a packet set, the Edit Packet Set dialog to select or insert a packet definition, and the Edit Packet dialog to define repetitive packet characteristics. In this dialog the "Packet Group" entry allows similar packets to automatically stop others in the same group when started (similar to "Radio Button" selection, in which only one item can be selected).

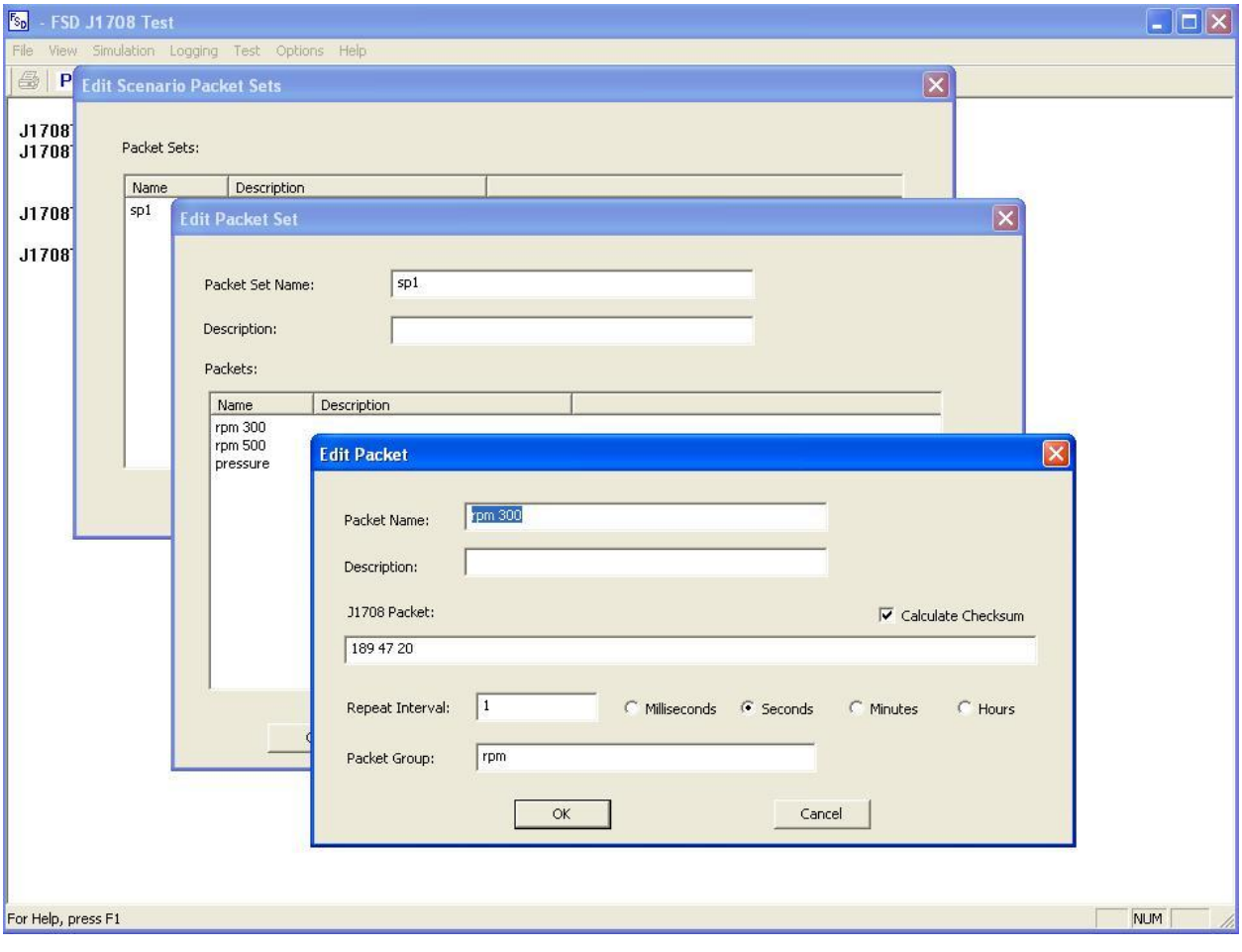


Figure 9: Scenario Packet Definition

Figure 10 shows scenario script configuration. To configure a simulation script, from the Simulation menu choose Define Scenario Scripts. The Edit Simulation Scripts dialog is used to select or insert scenario script file configurations. The Edit Script dialog provides the same options as described above for simulation scripts.

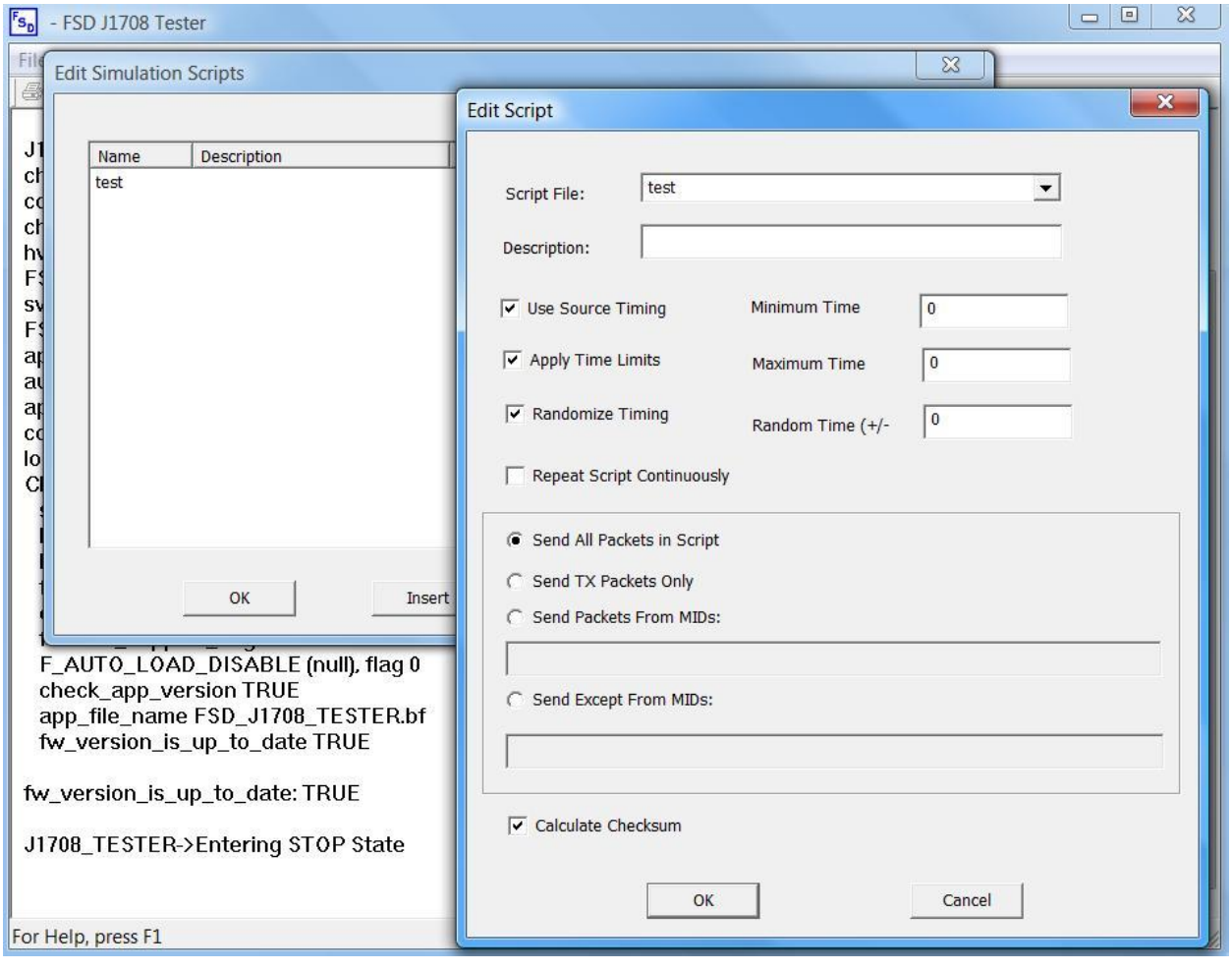


Figure 10: Scenario Script Definition

Figure 11 shows the dialogs used for defining scenarios and their time frame sequences. To configure a simulation script, from the Simulation menu choose Define Scenarios. The Edit Simulation Scenarios dialog is used to select or insert a scenario definition. The Edit Scenario dialog is used to select or insert a time frame within the scenario. The Edit Time Frame dialog is used to set the duration of the frame, and to define the set of repetitive packets and / or scripts affected by the time frame. The Edit Frame Item Options dialog is used to select a previously defined packet or script, and controls whether the packet or script is active (only) throughout the time frame, is started or stopped by the frame, or if a packet is started as a member of a packet group (stopping any other repetitive packet in the same group).

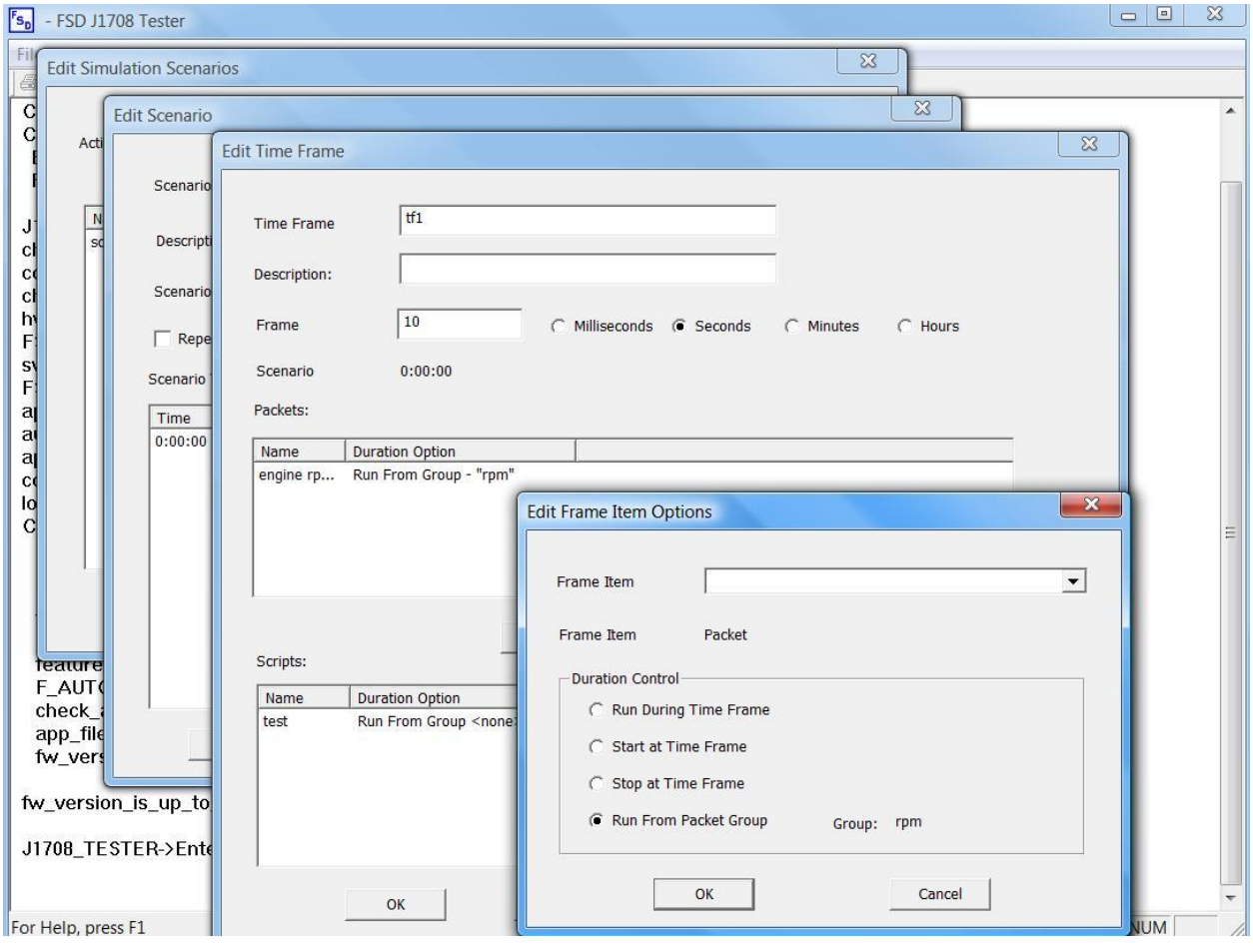


Figure 11: Scenario Time Frame Definition

The dialog shown in Figure 12 is used to select a defined scenario to be the active scenario when scenario simulation is enabled.

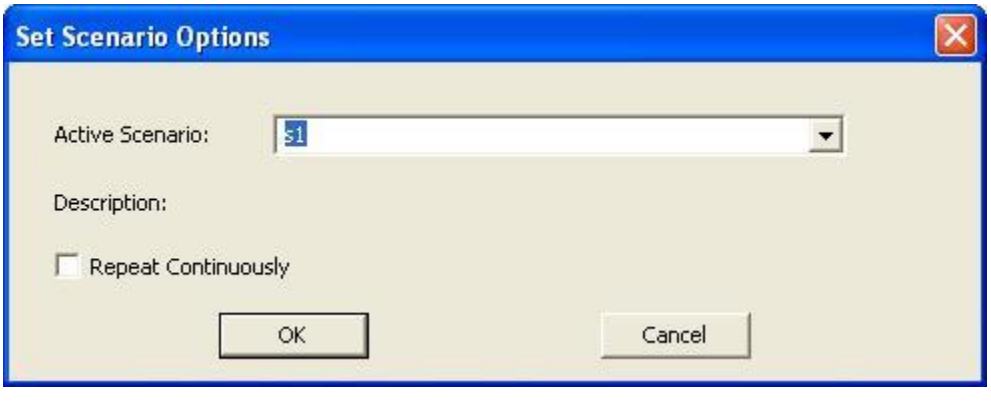


Figure 12: Active Scenario Selection

Customization Options:

FSD can add custom test features to the FSD J1708 Tester to simplify device testing and system integration for a device of interest. Typical customization options include adding device-specific packet generation to the "Predefined Packets" menu. To configure a simulation script, from the Test menu choose Predefined Packets. Figure 13 shows a packet generation example for one device type. Another potentially desirable option is custom decoding of manufacturer defined device specific packet information in PID 254 and/or PID 510 packets.

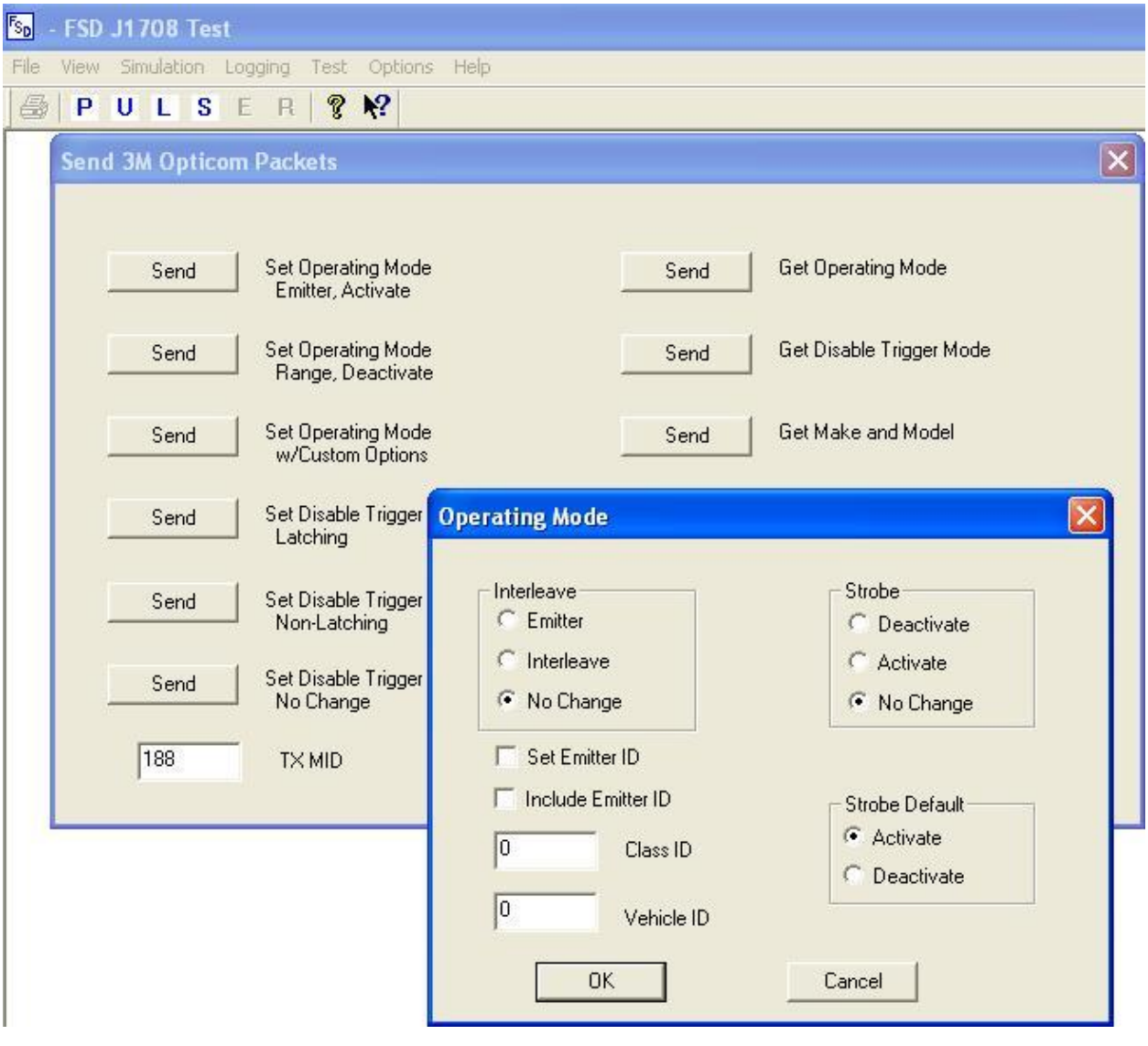


Figure 13: Custom Test Packet Generation Example

System Configuration Options:

Under the Options menu a set of configuration dialogs configure run-time system options such as which communications port to use. For most J1708 Tester users, the default options are appropriate. Normally the system finds the correct comm port automatically.

Use the “Check For Updates” feature to retrieve software and firmware updates via the Internet.

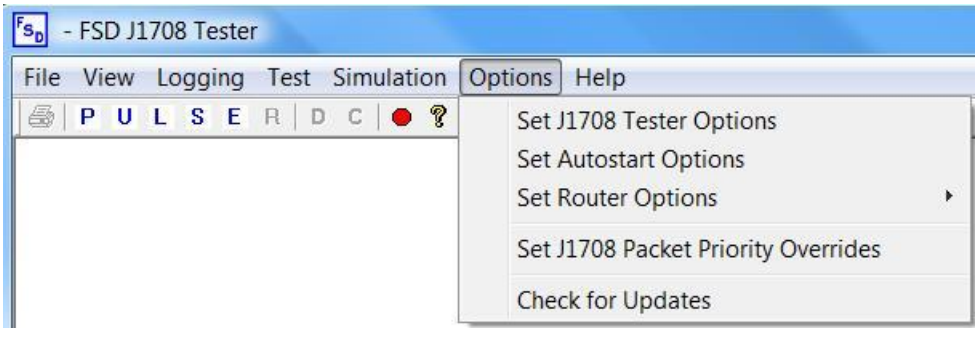


Figure 14: Configuration Options Menu

FSD J1708 Bridge Operation Guide

Configure Bridge Control Info List:

With the FSD J1708 Bridge to configure the control information choose from the View menu -> Bridge Control Editor, which opens the FSD J1708 Control application.

Bridge Control Info List:

From the Options menu of the FSD J1708 Control application, select Configure Bridge Control to display the Bridge Control Info List box, as shown in Figure 1. From the Profile drop list, select the profile to edit control information. If none is configured, the default profile is used (to configure profiles see the Configure Bridge Profiles section).

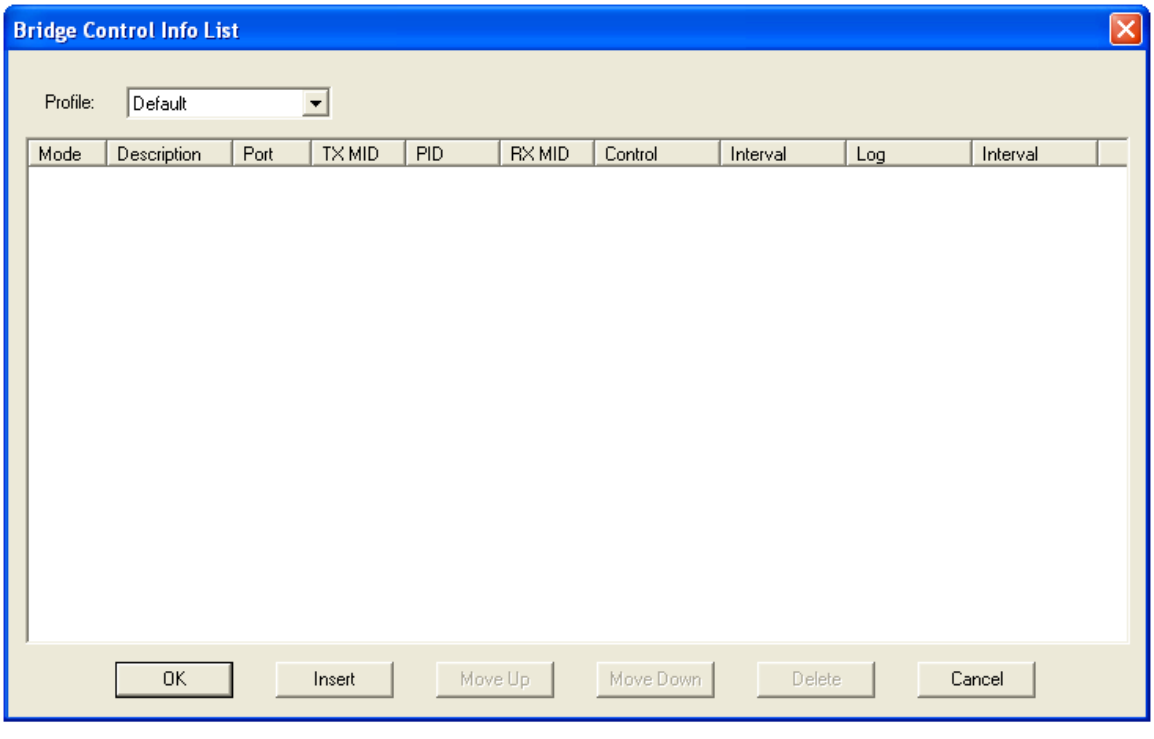


Figure 1: Bridge Control Info List

Click the Insert button to add entries to the control list. The top line listed in figure 2 shows the default entry when a new entry is inserted. Double clicking on a line displays the bride control options dialog (Figure 3).

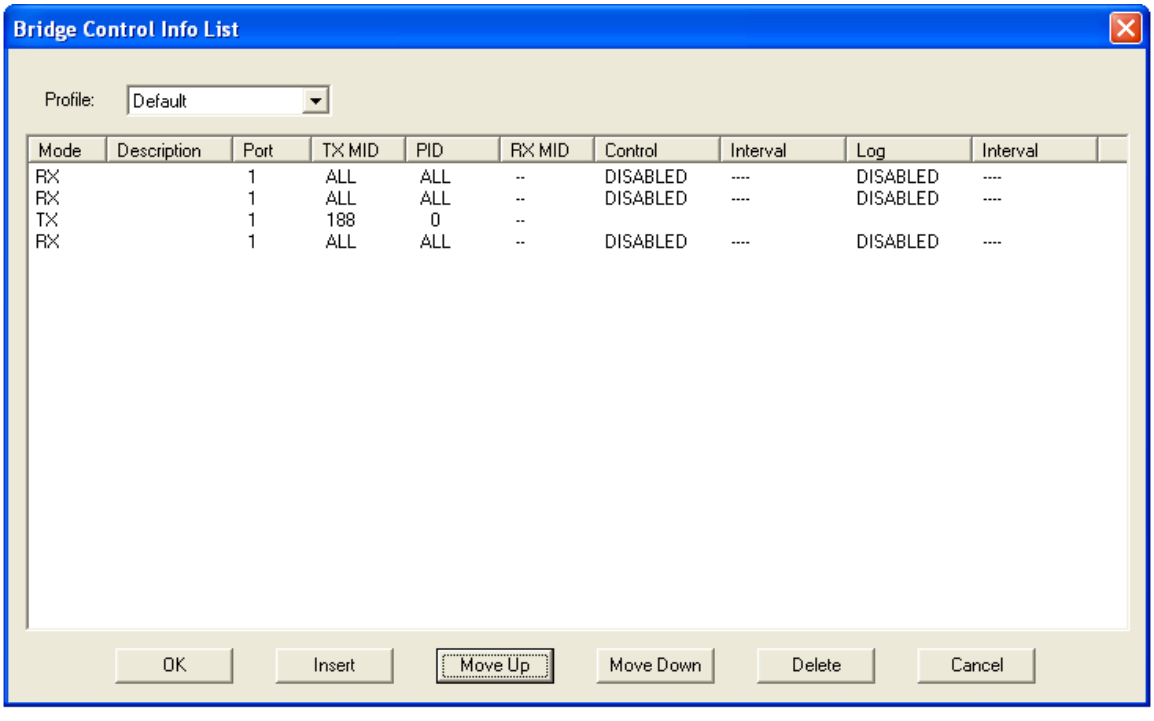


Figure 2: Populated Bridge Control Info List.

Edit Bridge Control Entry, Receive Mode

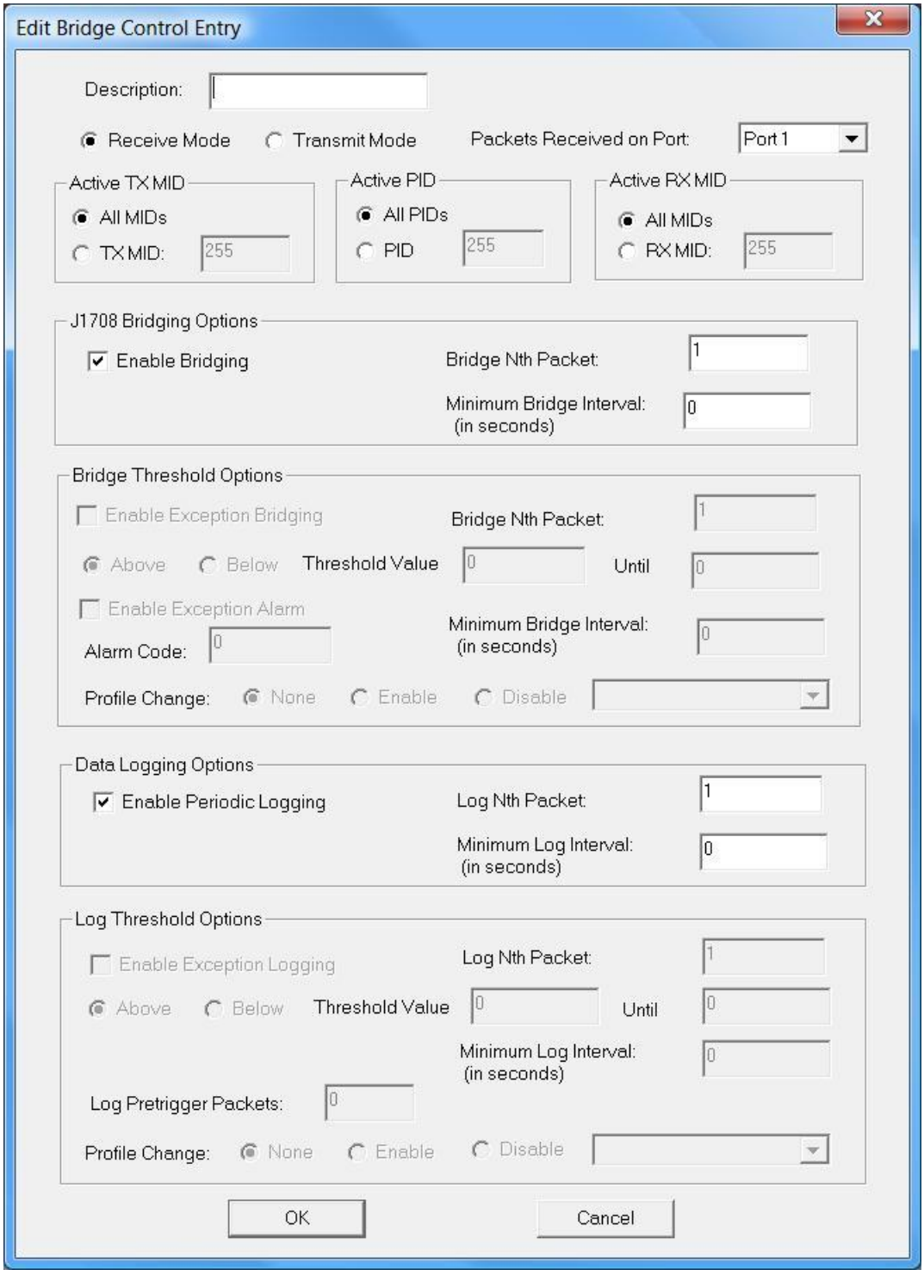


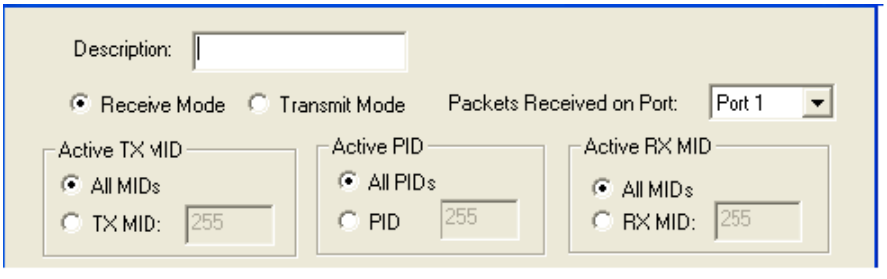
Figure 3: Edit Bridge Control Entry, Receive Mode

The following refers to the “Edit Bridge Control Entry” with "Receive Mode” selected. One can pick the J1708 packets to be bridged and logged (packet filter) by stipulating all or specific MIDs and/or PIDs.

The next sections configure Control Entry:

- J1708 Bridging Options
- Bridge Threshold Options
- Data Logging Options
- Log Threshold Options

While the different sections work independently, multiple sections may be enabled for the same packet filtering control.



Bridge Control Entry, Packet Filter Section

Figure 4: Bridge Control Entry, Packet Filter Section

Description:

Use this text box to describe the particular control entry.

Receive Mode / Transmit Mode Radio Button:

Determines whether this control entry controls incoming (receive) packets or outgoing (transmit) packets.

Packets Received on Port:

Select the port used for this control entry to filter packets.

Active TX MID:

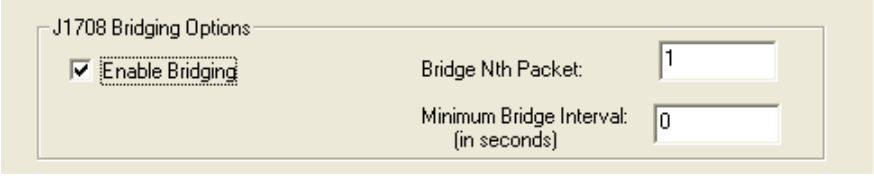
Specify the Transmitter MID that the control entry will act on these packets.

Active PID:

Enter the PID that the control entry will act on these packets.

Active RX MID:

This option is valid only for PIDs 254, 510, and 511. The control entry will act on the packets with the specified receiver's MID.



Bridge Control Entry, J1708 Bridging Options

Figure 5: Bridge Control Entry, J1708 Bridging Options

Enable Bridging:

With the Enable Bridging checkbox selected, the control entry bridges J1708 packets received on the selected port to the second port (configured in packet filtering section).

Bridge Nth Packet:

Every Nth packet that matches the packet filtering criteria is bridged from the chosen receive port to the second port.

For example:

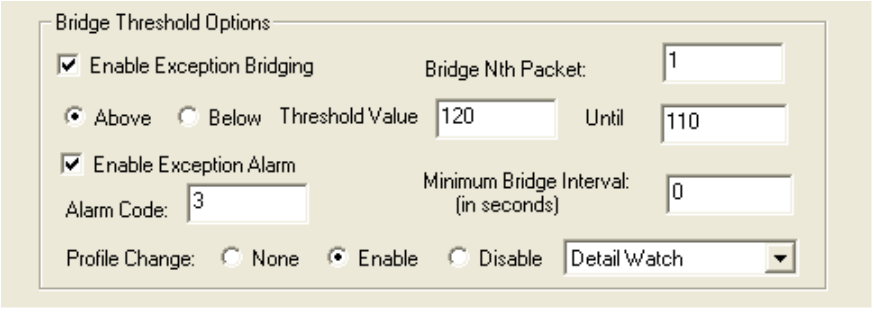
- Bridge Nth Packet = 1, each packet that matches the packet filtering conditions is bridged.
- Bridge Nth Packet = 2, every other packet that matches the packet filtering conditions is bridged.
- Bridge Nth Packet = 7, every seventh packet that matches the packet filtering conditions is bridged.

Minimum Bridge Interval:

The minimum bridge interval places timing restrictions on the Nth packet bridging.

For example:

- Minimum Bridge Interval = 0, No timing restrictions, packets are bridged based on the Bridge Nth Packet setting.
- Minimum Bridge Interval = 1, The Bridge Nth Packet setting is used if 1 second has passed since the last packet was bridged.
- Minimum Bridge Interval = 20, The Bridge Nth Packet setting is used if 20 seconds has passed since the last packet was bridged.



Bridge Control Entry, Bridge Threshold Options

Figure 6: Bridge Control Entry, Bridge Threshold Options

Enable Exception Bridging:

The enable exception bridging option allows bridging of packets based on the value of the datum contained in the J1708 packet.

Bridge Nth Packet:

Every Nth packet, which matches the packet filtering options and the threshold options, is bridged from the selected receive port to the second port.

For example:

- Bridge Nth Packet = 1, each packet that matches the packet filtering and threshold options is bridged.
- Bridge Nth Packet = 2, every other packet that matches the packet filtering and threshold options is bridged.
- Bridge Nth Packet = 5, every fifth packet that matches the packet filtering and threshold options is bridged.

Minimum Bridge Interval:

The minimum bridge interval places timing restrictions on the Nth packet bridging.

For example:

- Minimum Bridge Interval = 0, No timing restrictions, packets are bridged based on the Bridge Nth Packet setting.
- Minimum Bridge Interval = 1, The Bridge Nth Packet setting is used if 1 second has passed since the last packet was bridged.
- Minimum Bridge Interval = 20, The Bridge Nth Packet setting is used if 20 seconds has passed since the last packet was bridged.

Above/Below:

Choose whether the bridging criterion trips above or below the Threshold Value entered.

Threshold Value:

The threshold value is compared with the J1708 packet datum to execute an exception.

Until Value:

The Until value works as a hysteresis value. The threshold value generates the exception and the Until value reverses the exception.

Example: PID = 84, Threshold Value above 120

- Until Value = 120, Packets are bridged when the packet value exceeds 120 and continues bridging until the packet value drops below 120.
- Until Value = 110, The FSD J1708 bridge bridges PID 84 packets when the packet value exceeds 120 and continues bridging until the packet value drops below 110.

Enable Exception Alarm:

With Enable Exception Alarm checked, a J1708 packet, which causes an exception, will be bridged with a special alarm code added to the packet header. This feature results in a quick notification, when an exception is triggered.

An alarm packet is sent when the exception is triggered and additional alarm packets are sent if the exception value increases.

Example: PID = 84, Above Threshold value = 120, Until Value = 110

> An alarm packet is sent when the PID 84 data value hits 121. An additional alarm packet is sent each time the PID 84 data value increases. The alarm peak level is reset once the PID 84 datum reaches the Until Value, in this case 110.

If “Enabled Flash Log” is checked in the Configure Bridge Options menu, special alarm packets are also logged in the flash.

Alarm Code:

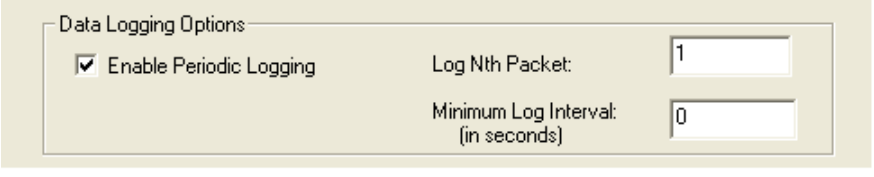
The alarm code can be set to 16 different alarm code values. (0 – 15)

Profile Change:

If multiple bridge control profiles were created, the profile change grouping allows enabling or disabling of different profiles based on exception criteria.

Thus, the user can monitor a specific variable, such as a vehicle's road speed. If a speed exception occurs the user could enable (or disable) a different profile that specifies monitoring of other parameters such as RPM, Oil Temp, or Engine Temp.

- None – No profile action is taken
- Enable – Enable the profile listed in the profile drop list box.
- Disable – Disable the profile listed in the profile drop list box.



Bridge Control Entry, Data Logging Options

Figure 7: Bridge Control Entry, Data Logging Options

Enable Periodic Logging:

If Enable Periodic Logging is selected, this control entry logs J1708 packets received on the selected port, based on the packet filtering options specified.

Log Nth Packet:

Every Nth packet that matches the packet filtering options is logged from the selected receive port.

For example:

- Log Nth Packet = 1, each packet that matches the packet filtering options is logged.
- Log Nth Packet = 2, every other packet that matches the packet filtering options is logged.
- Log Nth Packet = 8, every eighth packet that matches the packet filtering options is logged.

Minimum Log Interval:

The minimum log interval places timing restrictions on the Nth packet logging. For example:

- Minimum Log Interval = 0, No timing restrictions, packets are logged based on the Log Nth Packet setting.
- Minimum Log Interval = 1, The Log Nth Packet setting is used, if 1 second has passed since the last packet was logged.
- Minimum Log Interval = 20, The Log Nth Packet setting is used, if 20 seconds have passed since the last packet was logged.

Bridge Control Entry, Data Logging Options

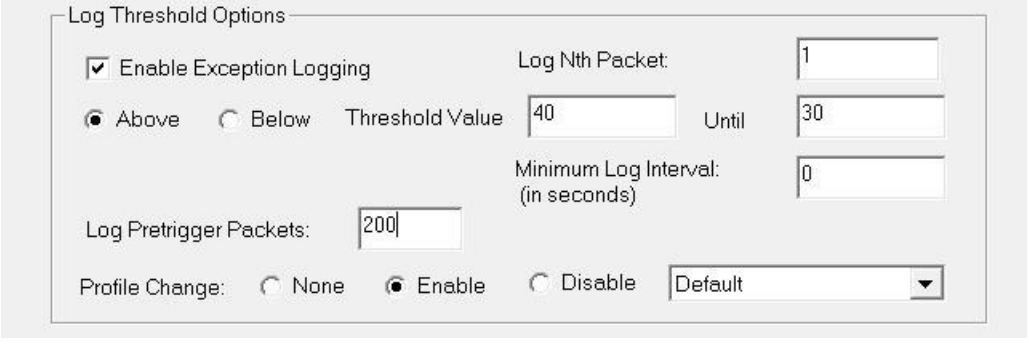


Figure 8: Bridge Control Entry, Data Logging Options

Enable Exception Logging:

The exception logging allows packets to be logged based on the datum value contained in the J1708 packet.

Log Nth Packet:

Every Nth packet that matches the packet filtering criteria and the threshold value is logged from the selected receive port. For example:

- Log Nth Packet = 1, each packet that matches the packet filtering and threshold options is logged.
- Log Nth Packet = 2, every other packet that matches the packet filtering and threshold options is logged.
- Log Nth Packet = 9, every ninth packet that matches the packet filtering and threshold options is logged.

Minimum Log Interval:

The minimum log interval places timing restrictions on the Nth packet logging.

For example:

- Minimum Log Interval = 0, No timing restrictions, packets are logged based on the Log Nth Packet setting.
- Log Bridge Interval = 1, The Log Nth Packet setting is used if 1 second has passed since the last packet was logged.
- Minimum Log Interval = 20, The Log Nth Packet setting is used only if 20 seconds has passed since the last packet was logged.

Above/Below:

Choose whether the packet is logged when the datum is above or below the Threshold Value.

Threshold Value:

The threshold value is used to compare the J1708 packet datum to execute an exception.

Until Value:

The Until value acts as a hysteresis. When reached, the threshold value generates the exception and the Until value reverses the exception.

Example: PID = 84, Above Threshold Value = 40

- Until Value = 40, Packets are logged if the packet value exceeds 40 and packets continually logged until the packet value drops below 40.
- Until Value = 30, The FSD J1708 bridge begins logging PID 84 packets once the packet data value exceeds 40 and continues to log PID 84 packets until the packet data value drops below 30.

Log Pretrigger Packets:

Enter a value from 0 to 200, which indicate the number of packets that are logged just prior to the trigger.

Profile Change:

If multiple bridge control profiles were created, the profile change grouping allows enabling or disabling of different profiles based on exception criteria.

Thus, the user can monitor a specific variable, such as a vehicle's road speed. If a speed exception occurs the user could enable (or disable) a different profile that specifies monitoring of other parameters such as RPM, Oil Temp, or Engine Temp.

- None – No profile action is taken
- Enable – Enable the profile listed in the profile drop list box.
- Disable – Disable the profile listed in the profile drop list box.

Edit Bridge Control Entry, Transmit Mode

When "Transmit Mode" is selected in the Edit Bridge Control Entry dialog box, the Edit Transmit Control Entry dialog is displayed. (Figure 9)

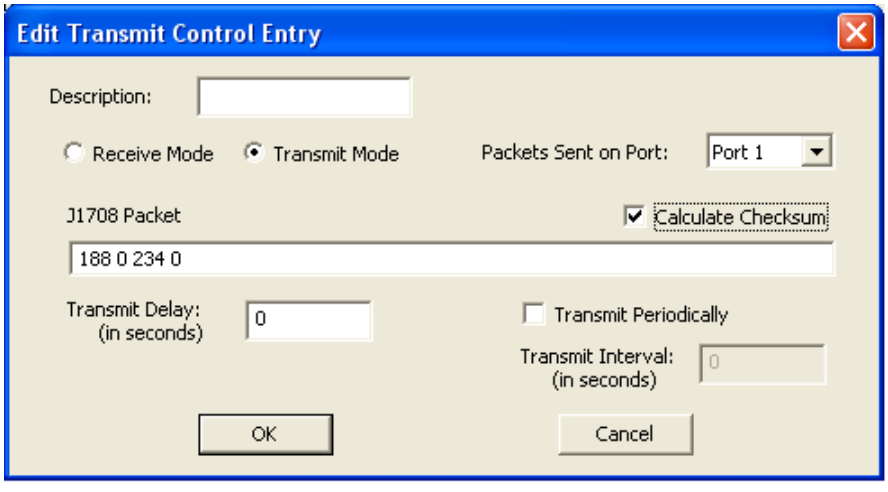


Figure 9: Edit Bridge Control Entry, Transmit Mode

If you need to monitor packets that are not typically broadcast, the Transmit Control Entry allows users to define transmit packets such as PID 0 request packets.

Description:

Enter text box to describe the particular control entry.

Receive Mode / Transmit Mode Radio Button:

The user selects the radio button to designate this control entry to control either incoming (receive) packets or outgoing (transmit) packets. Selecting Receive Mode reverts to the "Edit Bridge Control Entry" dialog (Fig. 3).

Packets Sent on Port:

Select the port used to transmit the J1708 packet.

J1708 Packet:

Enter the J1708 packet, in decimal format.

Calculate Checksum:

Select the calculate checksum, if you want the control entry to calculate the J1708 packet checksum automatically. Insert a placeholder value at the end of the packet for the checksum.

Transmit Interval:

Valid Range: (0 – 65535).

If Transmit Periodically is enabled, the entered value dictates how often the packet is transmitted.

Transmit Delay:

Valid Range: (0 – 65535).

The transmit delay specifies the time period before transmitting the packet, after the controller powers up or profile is enabled.

Transmit Periodically:

Select transmit periodically to send the packet every “Transmit Interval” after the transmit delay time has passed.

FSD J1708 Logger Operation Guide

The FSD J1708 Logger is similar to the FSD J1708 Bridge, but addition has the components to log packets communicated to the vehicle's J1708 bus.

Configure Bridge Control Info List:

With the FSD J1708 Logger, one needs to configure the control information for the Bridge portion of the logger. Choose from the View menu -> Bridge Control Editor, which opens the FSD J1708 Control application.

Bridge Control Info List:

From the Options menu of the FSD J1708 Control application, select Configure Bridge Control to display the Bridge Control Info List box, as shown in Figure 1. From the Profile drop list, select the profile to edit control information. If none is configured, the default profile is used (to configure profiles see the Configure Bridge Profiles section).

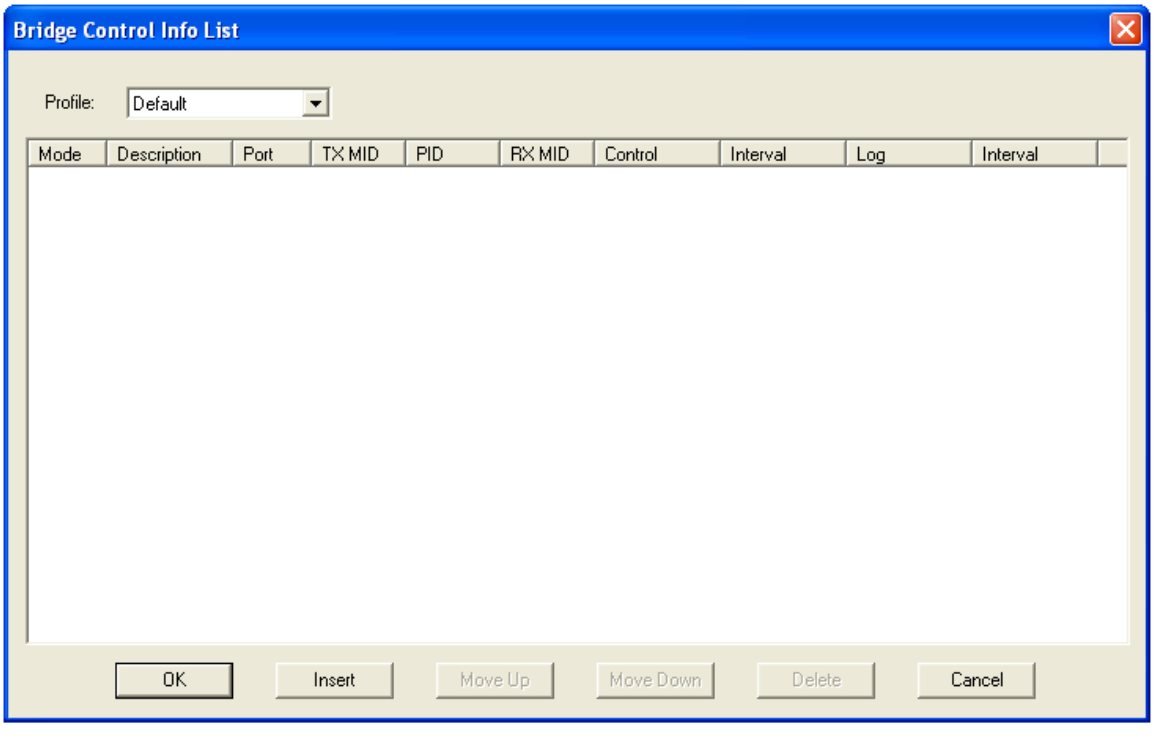


Figure 1: Bridge Control Info List

Click the Insert button to add entries to the control list. The top line listed in figure 2 shows the default entry when a new entry is inserted. Double clicking on a line displays the bride control options dialog (Figure 3).

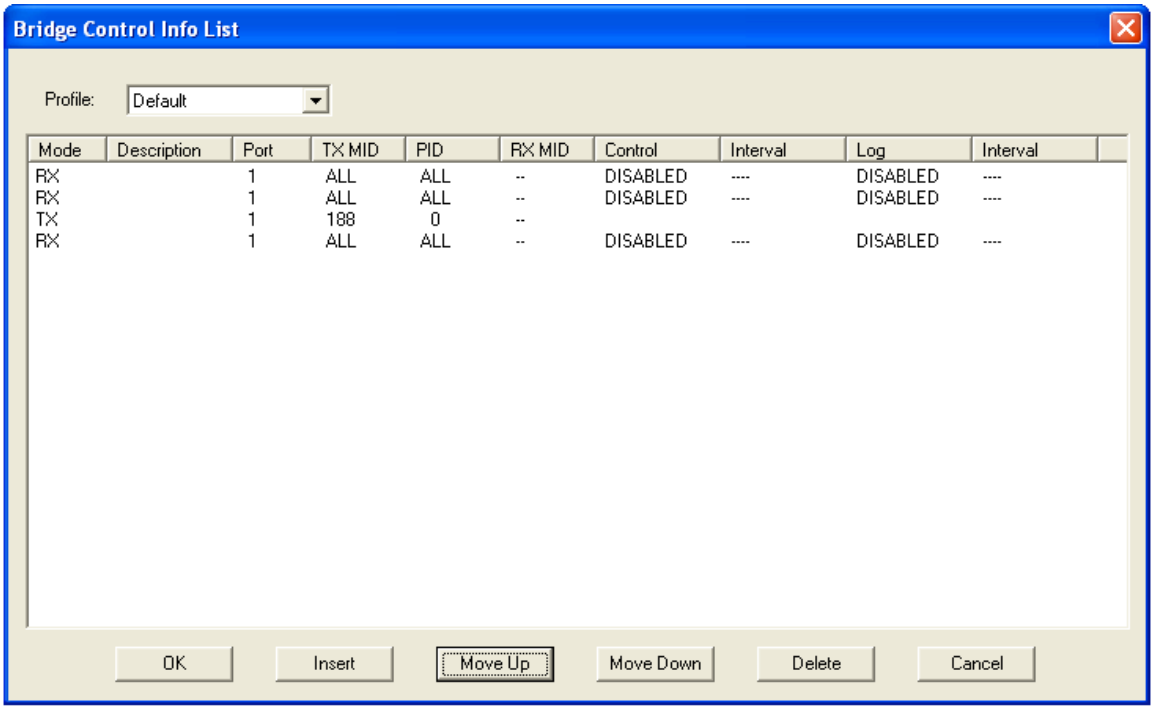


Figure 2: Populated Bridge Control Info List.

Edit Bridge Control Entry, Receive Mode

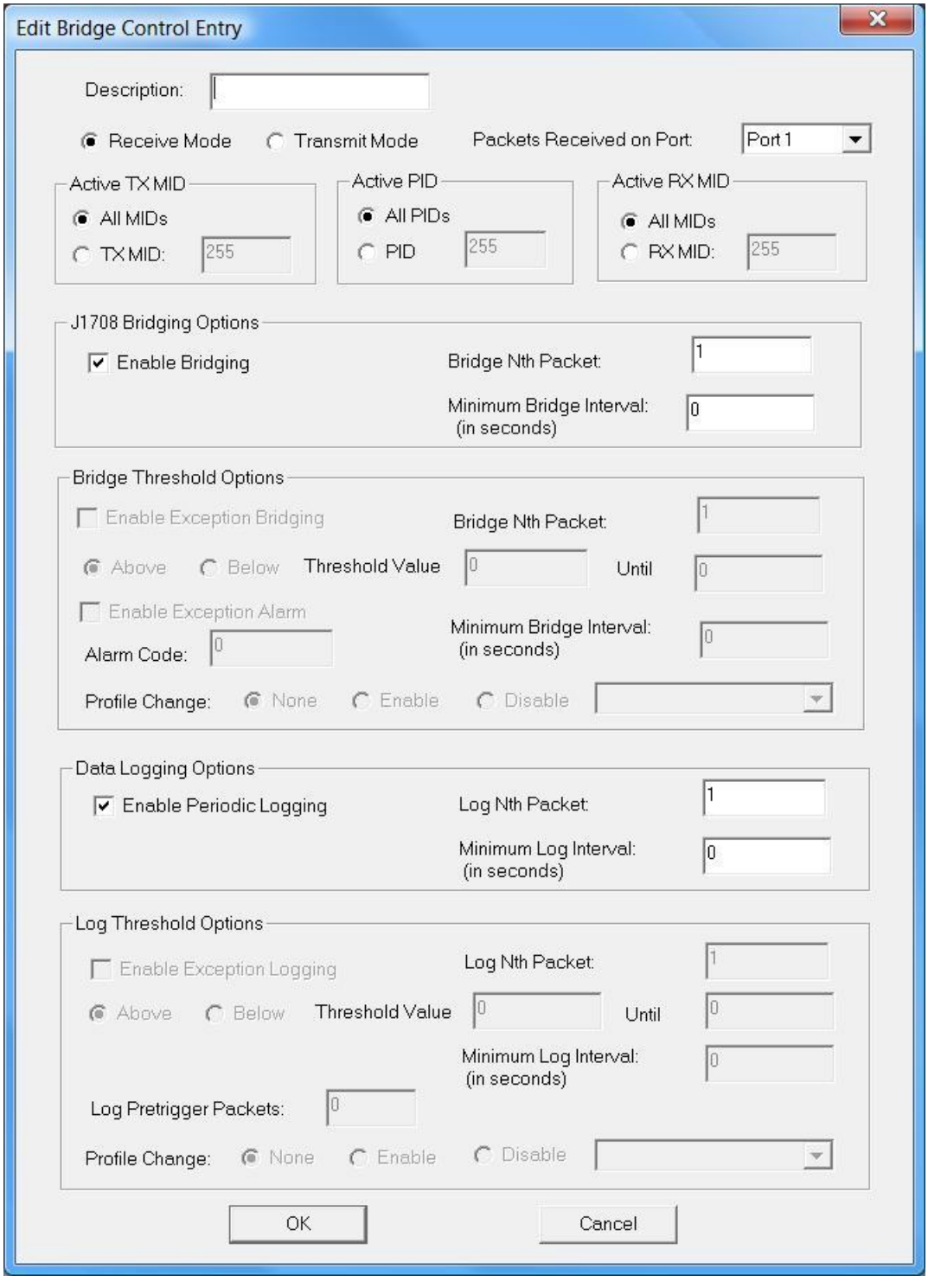


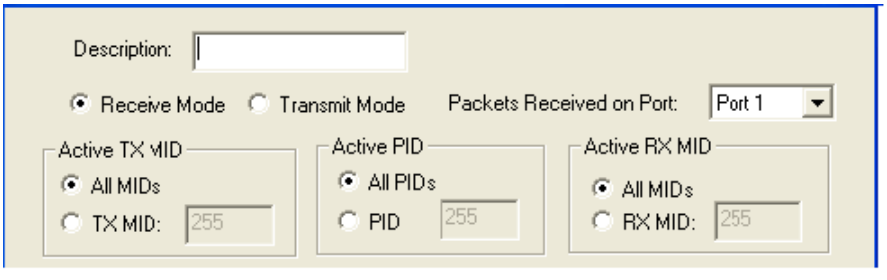
Figure 3: Edit Bridge Control Entry, Receive Mode

The following refers to the “Edit Bridge Control Entry” with "Receive Mode” selected. One can pick the J1708 packets to be bridged and logged (packet filter) by stipulating all or specific MIDs and/or PIDs.

The next sections configure Control Entry:

- J1708 Bridging Options
- Bridge Threshold Options
- Data Logging Options
- Log Threshold Options

While the different sections work independently, multiple sections may be enabled for the same packet filtering control.



Bridge Control Entry, Packet Filter Section

Figure 4: Bridge Control Entry, Packet Filter Section

Description:

Use this text box to describe the particular control entry.

Receive Mode / Transmit Mode Radio Button:

Determines whether this control entry controls incoming (receive) packets or outgoing (transmit) packets.

Packets Received on Port:

Select the port used for this control entry to filter packets.

Active TX MID:

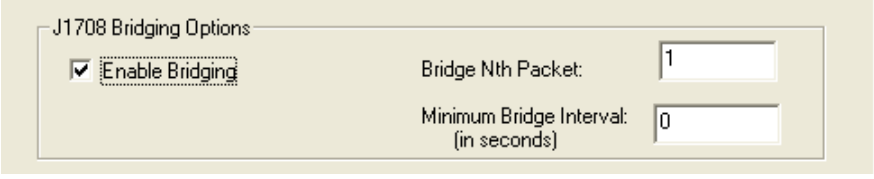
Specify the Transmitter MID that the control entry will act on these packets.

Active PID:

Enter the PID that the control entry will act on these packets.

Active RX MID:

This option is valid only for PIDs 254, 510, and 511. The control entry will act on the packets with the specified receiver's MID.



Bridge Control Entry, J1708 Bridging Options

Figure 5: Bridge Control Entry, J1708 Bridging Options

Enable Bridging:

With the Enable Bridging checkbox selected, the control entry bridges J1708 packets received on the selected port to the second port (configured in packet filtering section).

Bridge Nth Packet:

Every Nth packet that matches the packet filtering criteria is bridged from the chosen receive port to the second port.

For example:

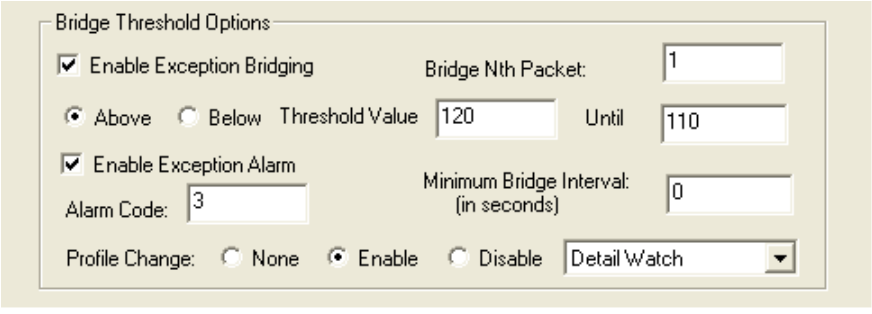
- Bridge Nth Packet = 1, each packet that matches the packet filtering conditions is bridged.
- Bridge Nth Packet = 2, every other packet that matches the packet filtering conditions is bridged.
- Bridge Nth Packet = 7, every seventh packet that matches the packet filtering conditions is bridged.

Minimum Bridge Interval:

The minimum bridge interval places timing restrictions on the Nth packet bridging.

For example:

- Minimum Bridge Interval = 0, No timing restrictions, packets are bridged based on the Bridge Nth Packet setting.
- Minimum Bridge Interval = 1, The Bridge Nth Packet setting is used if 1 second has passed since the last packet was bridged.
- Minimum Bridge Interval = 20, The Bridge Nth Packet setting is used if 20 seconds has passed since the last packet was bridged.



Bridge Control Entry, Bridge Threshold Options

Figure 6: Bridge Control Entry, Bridge Threshold Options

Enable Exception Bridging:

The enable exception bridging option allows bridging of packets based on the value of the datum contained in the J1708 packet.

Bridge Nth Packet:

Every Nth packet, which matches the packet filtering options and the threshold options, is bridged from the selected receive port to the second port.

For example:

- Bridge Nth Packet = 1, each packet that matches the packet filtering and threshold options is bridged.
- Bridge Nth Packet = 2, every other packet that matches the packet filtering and threshold options is bridged.
- Bridge Nth Packet = 5, every fifth packet that matches the packet filtering and threshold options is bridged.

Minimum Bridge Interval:

The minimum bridge interval places timing restrictions on the Nth packet bridging.

For example:

- Minimum Bridge Interval = 0, No timing restrictions, packets are bridged based on the Bridge Nth Packet setting.
- Minimum Bridge Interval = 1, The Bridge Nth Packet setting is used if 1 second has passed since the last packet was bridged.
- Minimum Bridge Interval = 20, The Bridge Nth Packet setting is used if 20 seconds has passed since the last packet was bridged.

Above/Below:

Choose whether the bridging criterion trips above or below the Threshold Value entered.

Threshold Value:

The threshold value is compared with the J1708 packet datum to execute an exception.

Until Value:

The Until value works as a hysteresis value. The threshold value generates the exception and the Until value reverses the exception.

Example: PID = 84, Threshold Value above 120

- Until Value = 120, Packets are bridged when the packet value exceeds 120 and continues bridging until the packet value drops below 120.
- Until Value = 110, The FSD J1708 bridge bridges PID 84 packets when the packet value exceeds 120 and continues bridging until the packet value drops below 110.

Enable Exception Alarm:

With Enable Exception Alarm checked, a J1708 packet, which causes an exception, will be bridged with a special alarm code added to the packet header. This feature results in a quick notification, when an exception is triggered.

An alarm packet is sent when the exception is triggered and additional alarm packets are sent if the exception value increases.

Example: PID = 84, Above Threshold value = 120, Until Value = 110

> An alarm packet is sent when the PID 84 data value hits 121. An additional alarm packet is sent each time the PID 84 data value increases. The alarm peak level is reset once the PID 84 datum reaches the Until Value, in this case 110.

If “Enabled Flash Log” is checked in the Configure Bridge Options menu, special alarm packets are also logged in the flash.

Alarm Code:

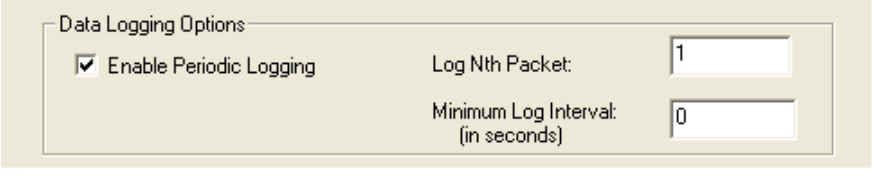
The alarm code can be set to 16 different alarm code values. (0 – 15)

Profile Change:

If multiple bridge control profiles were created, the profile change grouping allows enabling or disabling of different profiles based on exception criteria.

Thus, the user can monitor a specific variable, such as a vehicle's road speed. If a speed exception occurs the user could enable (or disable) a different profile that specifies monitoring of other parameters such as RPM, Oil Temp, or Engine Temp.

- None – No profile action is taken
- Enable – Enable the profile listed in the profile drop list box.
- Disable – Disable the profile listed in the profile drop list box.



Bridge Control Entry, Data Logging Options

Figure 7: Bridge Control Entry, Data Logging Options

Enable Periodic Logging:

If Enable Periodic Logging is selected, this control entry logs J1708 packets received on the selected port, based on the packet filtering options specified.

Log Nth Packet:

Every Nth packet that matches the packet filtering options is logged from the selected receive port.

For example:

- Log Nth Packet = 1, each packet that matches the packet filtering options is logged.
- Log Nth Packet = 2, every other packet that matches the packet filtering options is logged.
- Log Nth Packet = 8, every eighth packet that matches the packet filtering options is logged.

Minimum Log Interval:

The minimum log interval places timing restrictions on the Nth packet logging.

For example:

- Minimum Log Interval = 0, No timing restrictions, packets are logged based on the Log Nth Packet setting.
- Minimum Log Interval = 1, The Log Nth Packet setting is used, if 1 second has passed since the last packet was logged.

- Minimum Log Interval = 20, The Log Nth Packet setting is used, if 20 seconds have passed since the last packet was logged.

Bridge Control Entry, Data Logging Options

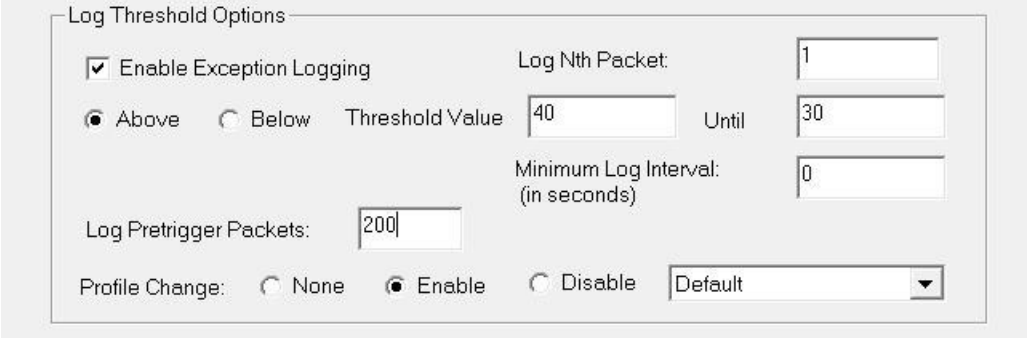


Figure 8: Bridge Control Entry, Data Logging Options

Enable Exception Logging:

The exception logging allows packets to be logged based on the datum value contained in the J1708 packet.

Log Nth Packet:

Every Nth packet that matches the packet filtering criteria and the threshold value is logged from the selected receive port.

For example:

- Log Nth Packet = 1, each packet that matches the packet filtering and threshold options is logged.
- Log Nth Packet = 2, every other packet that matches the packet filtering and threshold options is logged.
- Log Nth Packet = 9, every ninth packet that matches the packet filtering and threshold options is logged.

Minimum Log Interval:

The minimum log interval places timing restrictions on the Nth packet logging.

For example:

- Minimum Log Interval = 0, No timing restrictions, packets are logged based on the Log Nth Packet setting.

- Log Bridge Interval = 1, The Log Nth Packet setting is used if 1 second has passed since the last packet was logged.
- Minimum Log Interval = 20, The Log Nth Packet setting is used only if 20 seconds has passed since the last packet was logged.

Above/Below:

Choose whether the packet is logged when the datum is above or below the Threshold Value.

Threshold Value:

The threshold value is used to compare the J1708 packet datum to execute an exception.

Until Value:

The Until value acts as a hysteresis. When reached, the threshold value generates the exception and the Until value reverses the exception.

Example: PID = 84, Above Threshold Value = 40

- Until Value = 40, Packets are logged if the packet value exceeds 40 and packets continually logged until the packet value drops below 40.
- Until Value = 30, The FSD J1708 bridge begins logging PID 84 packets once the packet data value exceeds 40 and continues to log PID 84 packets until the packet data value drops below 30.

Log Pretrigger Packets:

Enter a value from 0 to 200, which indicate the number of packets that are logged just prior to the trigger.

Profile Change:

If multiple bridge control profiles were created, the profile change grouping allows enabling or disabling of different profiles based on exception criteria.

Thus, the user can monitor a specific variable, such as a vehicle's road speed. If a speed exception occurs the user could enable (or disable) a different profile that specifies monitoring of other parameters such as RPM, Oil Temp, or Engine Temp.

- None – No profile action is taken
- Enable – Enable the profile listed in the profile drop list box.
- Disable – Disable the profile listed in the profile drop list box.

Edit Bridge Control Entry, Transmit Mode

When "Transmit Mode" is selected in the Edit Bridge Control Entry dialog box, the Edit Transmit Control Entry dialog is displayed. (Figure 9)

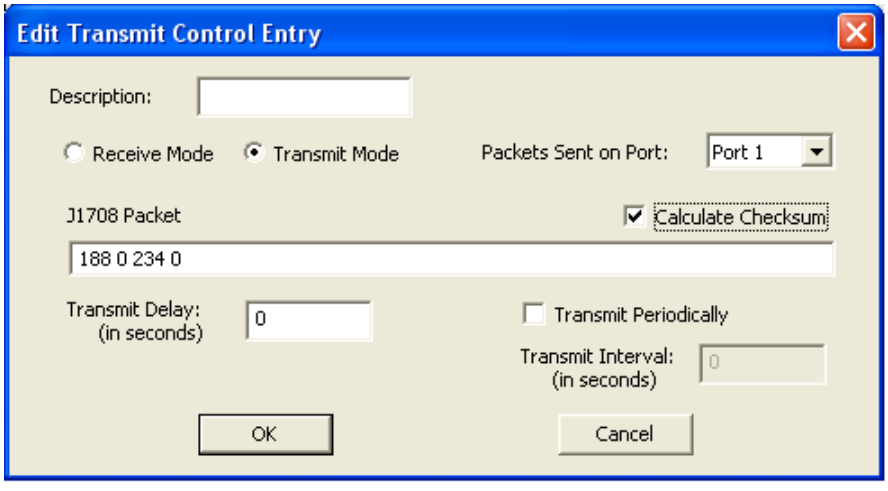


Figure 9: Edit Bridge Control Entry, Transmit Mode

If you need to monitor packets that are not typically broadcast, the Transmit Control Entry allows users to define transmit packets such as PID 0 request packets.

Description:

Enter text box to describe the particular control entry.

Receive Mode / Transmit Mode Radio Button:

The user selects the radio button to designate this control entry to control either incoming (receive) packets or outgoing (transmit) packets. Selecting Receive Mode reverts to the "Edit Bridge Control Entry" dialog (Fig. 3).

Packets Sent on Port:

Select the port used to transmit the J1708 packet.

J1708 Packet:

Enter the J1708 packet, in decimal format.

Calculate Checksum:

Select the calculate checksum, if you want the control entry to calculate the J1708 packet checksum automatically. Insert a placeholder value at the end of the packet for the checksum.

Transmit Interval:

Valid Range: (0 – 65535).

If Transmit Periodically is enabled, the entered value dictates how often the packet is transmitted.

Transmit Delay:

Valid Range: (0 – 65535).

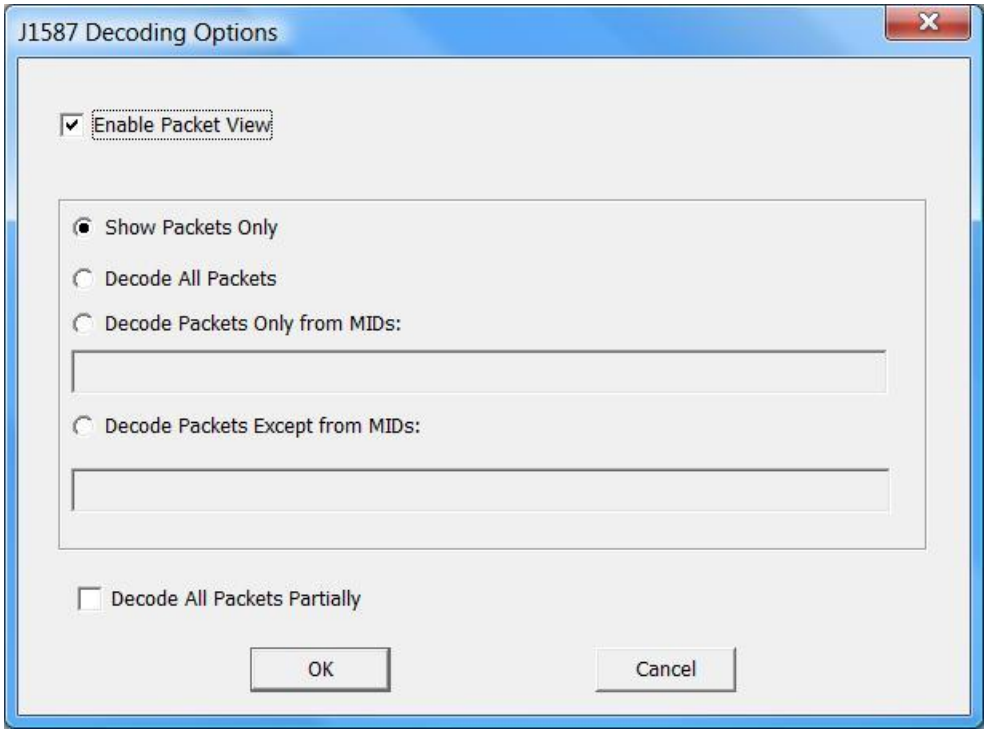
The transmit delay specifies the time period before transmitting the packet, after the controller powers up or profile is enabled.

Transmit Periodically:

Select transmit periodically to send the packet every “Transmit Interval” after the transmit delay time has passed.

J1587 Decoding Options

To specify how the logged packets are decoded in the report file. From the View menu choose J1587 Decoding Options.



Enable Packet View:

Selecting the packet view displays all decoding to the screen.

Show Packets Only:

Packet values are shown to the screen, without decoding of the packets.

Decode All Packets:

Fully decode all packets to the screen.

Decode Packets Only from MIDs:

All packets are displayed, but only packets from the listed MIDs are decoded.
Example List: “128 188 187”

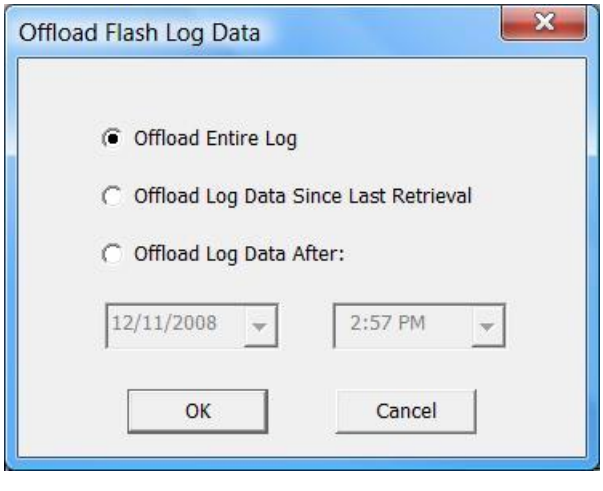
Decode Packets Except from MIDs:

All packets are displayed and decoded except packets with the listed MIDs.
Example List: “128 188 187”

Displaying Logged Packets

From the Logging menu choose Retrieve Flash Log. The following dialog appears.

Retrieve Flash Log Option Dialog



Select from the following options to download from the flash memory.

Offload Entire Log:

All data in the flash are retrieved.

Offload Log Data Since Last Retrieval:

Data, not previously retrieved, are retrieved.

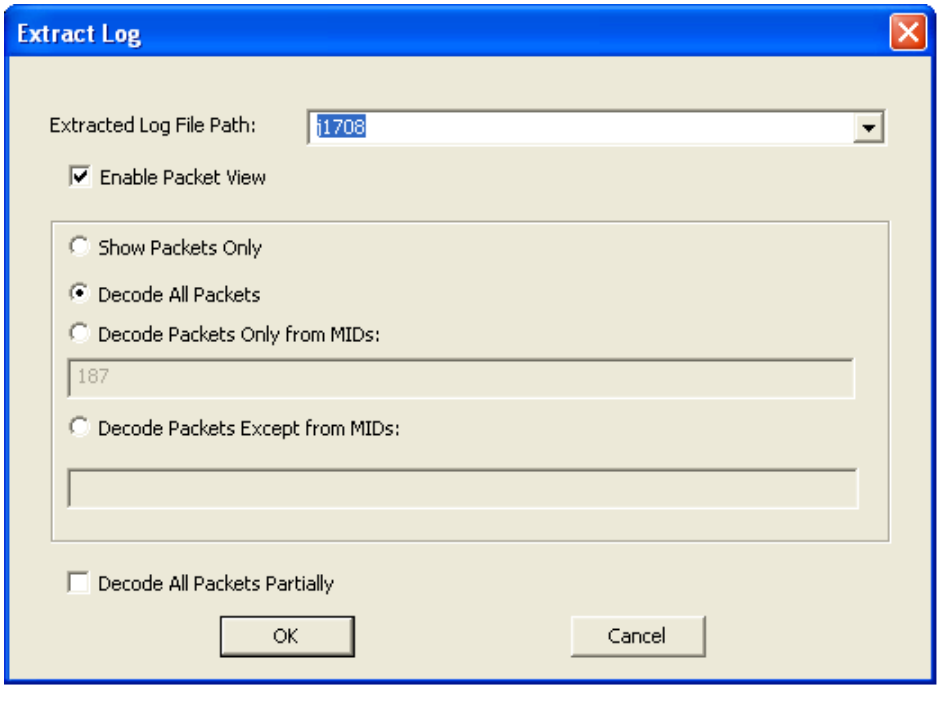
Offload Log Data After:

Data, stored after the specified date, are retrieved.

Click “OK”. A dialog appears to save the file with the file name (jt_flog extension) you assign.

Extract Flash Log Option Dialog

To display the log file, choose Extract Flash Log from the Logging menu. The following dialog appears.



Extracted Log File Path:

Select the file to extract. The file is stored in the J1708 software installation directory. The path is \<Your_Install_Directory>\data\.

Enable Packet View:

Enabling the packet view displayed all packets on the screen. When disabled, a “<” or “>” denotes a packet transmitted/received.

Show Packets Only:

Only packet values are extracted.

Decode All Packets:

Fully decode all packets.

Decode Packets Only from MIDs:

All packets are extracted, but only packets from the listed MIDs are decoded.
Example List: “128 188 187”

Decode Packets Except from MIDs:

All packets are extracted and decoded except packets with the listed MIDs.
Example List: “128 188 187”

FSD J1708 Control Software

J1708 Control Overview

J1708 Control is used to configure J1708 Bridge and/or J1708 Logger for control over J1708 packets received.

J1708 Control Menu:

File Menu Commands:

- Open: Open a J1708 Control file for editing (*.jt_bcfg)
- Save As: Save the current configuration under a new name.
- Print: Print the current Bridge Control Info List
- Print Preview
- Exit: Exit the J1708 Control program.

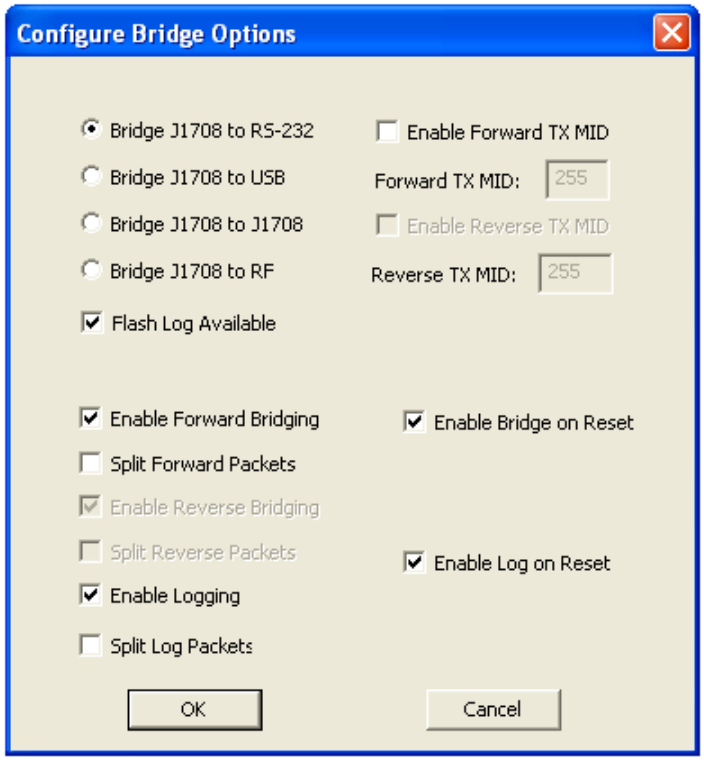
View Menu Commands:

- Toolbar: Turn on and off view of the toolbar
- Status Bar: Turn on and off view of the status bar.

Options Menu Commands:

- Configure Bridge Options: Open the global configuration dialog.
  See "Configure J1708 Bridge Options"
- Configure Data Version: Open the data version configuration dialog.
  See "Configure Data Version"
- Configure Profiles: Open the Profile configuration dialog.
  See "Configure J1708 Control Profile"
- Configure Bridge Control: Open the Bridge Control Info List dialog.
  See "Configure J1708 Bridge Control"
- Check for Updates: Over the internet, check for the latest software updates.

Configure J1708 Bridge Options



Bridging Types: Choose the radio button that indicates what hardware the J1708 input bridges to. Port1 to Port2

- "Bridge J1708 to RS-232"
- "Bridge J1708 to USB"
- "Bridge J1708 to J1708"
- "Bridge J1708 to RF"

Flash Log Available:

If the FSD J1708 Bridge is equipped with flash logging hardware, select the flash log available check box.

Enable Forward TX MID:

With the enable forward TX MID check box selected the FSD J1708 Bridge uses the assigned "Forward TX MID" when responding to requests or when transmitting J1708 packets that originate from the FSD J1708 Bridge on Port 1.

If unchecked, the FSD J1708 Bridge is “invisible” and neither responds to J1708 commands nor originates packets on Port 1.

Enable Reverse TX MID:

If the enable reverse TX MID check box is selected, the J1708 Bridge uses the assigned “Reverse TX MID” when responding to requests or transmitting J1708 packets, which originate from the FSD J1708 Bridge on Port 2.

If unchecked, the FSD J1708 Bridge is “invisible” and neither originates packets nor responds to J1708 commands on Port 2.

Enable Forward Bridging:

When the enable forward bridging check box is selected and bridging enabled, the FSD J1708 Bridge bridges J1708 packets from Port1 to Port2 based on the bridging type definitions. This occurs either at power up or by external command.

Split Forward Packets:

When the split forward packets check box is selected, the FSD J1708 Bridge splits packets with multi PIDs received from Port1 into their respective packets with single PID on Port2.

Enable Reverse Bridging:

When the enable reverse bridging check box is selected and bridging enabled, the FSD J1708 Bridge bridges J1708 packets from Port2 to Port1 based on the bridging type definitions. This occurs either at power up or by external command.

Split Reverse Packets:

When the split reverse packets check box is selected, the FSD J1708 Bridge splits packets with multi PIDs received from Port2 into their respective packets with single PID on Port1.

Enable Bridge on Reset:

When the enable bridge on reset check box is selected, the FSD J1708 Bridge begins bridging J1708 packets immediately upon power up.

Enable Logging:

With the enable logging check box checked, logging is enabled.

Split Log Packets:

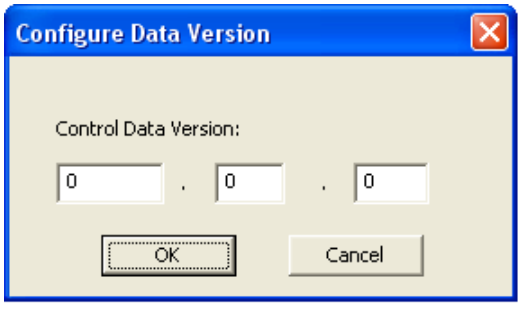
When the split log packets check box is selected, the FSD J1708 Bridge splits any valid multi PID packets into single PID packets prior to logging the data.

Enable Log on Reset:

When the “Enable Log on Reset” check box is selected along with the “Enable Logging” check box, the FSD J1708 Bridge begins logging valid J1708 packets immediately upon power up.

Configure Bridge Control Data Version:

Figure 1: Configure Data Version Dialog



The configure data version dialog is used to assign a data version to the current set of control variables being loaded into an FSD J1708 Bridge.

Configure Bridge Control Profile List:

In the FSD J1708 Control application, to configure the different profiles, from the Options menu select Configure Profiles, which opens the Configure Profiles dialog (Figure 1).

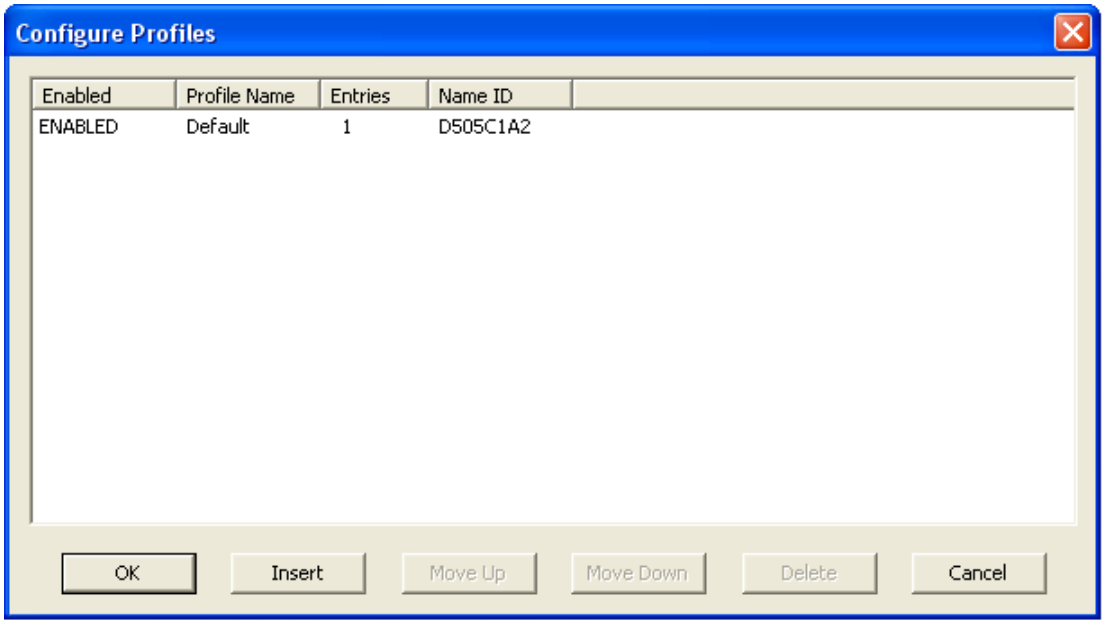


Figure 1: Configure Profiles Entry List

There is a default profile used for normal single profile control operations. Click the Insert button to add profiles.

Double clicking on a profile displays the Edit Profile Dialog box (Figure 2).

Edit Profile

Figure 2: Edit Profile Dialog Box

Profile Name:

Name used to describe this profile.

Name ID:

Profile specific ID assigned by the J1708 Control program.

Enable Profile on Reset:

Select this option to enable control entries associated with this profile when the FSD J1708 Bridge powers up.

Disable After Interval:

If the disable after interval option is chosen, the profile automatically disables after the number of seconds specified in the Disable Interval edit box. This interval starts when the controller powers up or when an exception event enables a profile (see exception bridging in the J1708 Control).

Disable Interval:

Enter a value in seconds that the profile is enabled after power up or by an exception event. Valid Range (0 – 65535).

FSD J1708 Control Application

In FSD J1708 Logger, to configure the control information for the Bridge, choose from the View menu -> Bridge Control Editor, which opens the FSD J1708 Control application.

Configure Bridge Control Info List:

From the Options menu of the FSD J1708 Control application, select Configure Bridge Control to display the Bridge Control Info List box, as shown in Figure 1. From the Profile drop list, select the profile to edit control information. If none is configured, the default profile is used (to configure profiles see the Configure Bridge Profiles section).

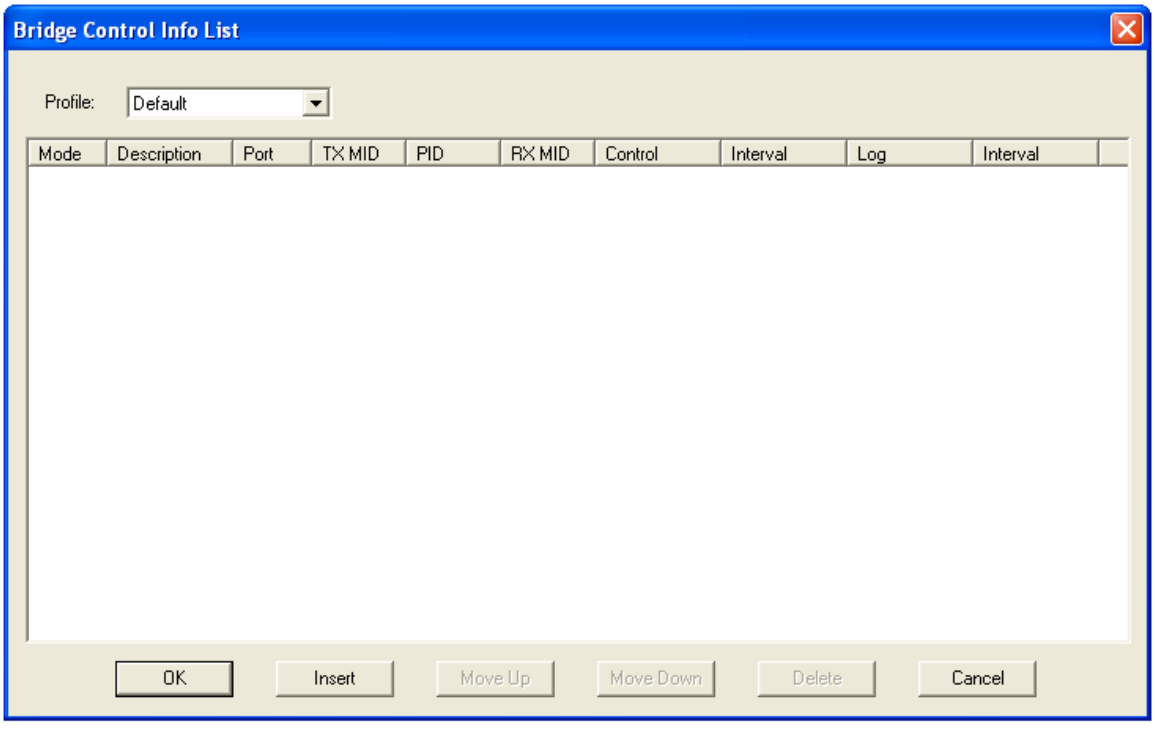


Figure 1: Bridge Control Info List

Click the Insert button to add entries to the control list. The top line listed in figure 2 shows the default entry when one inserts an entry. Double clicking on a line displays the bride control options dialog (Figure 3).

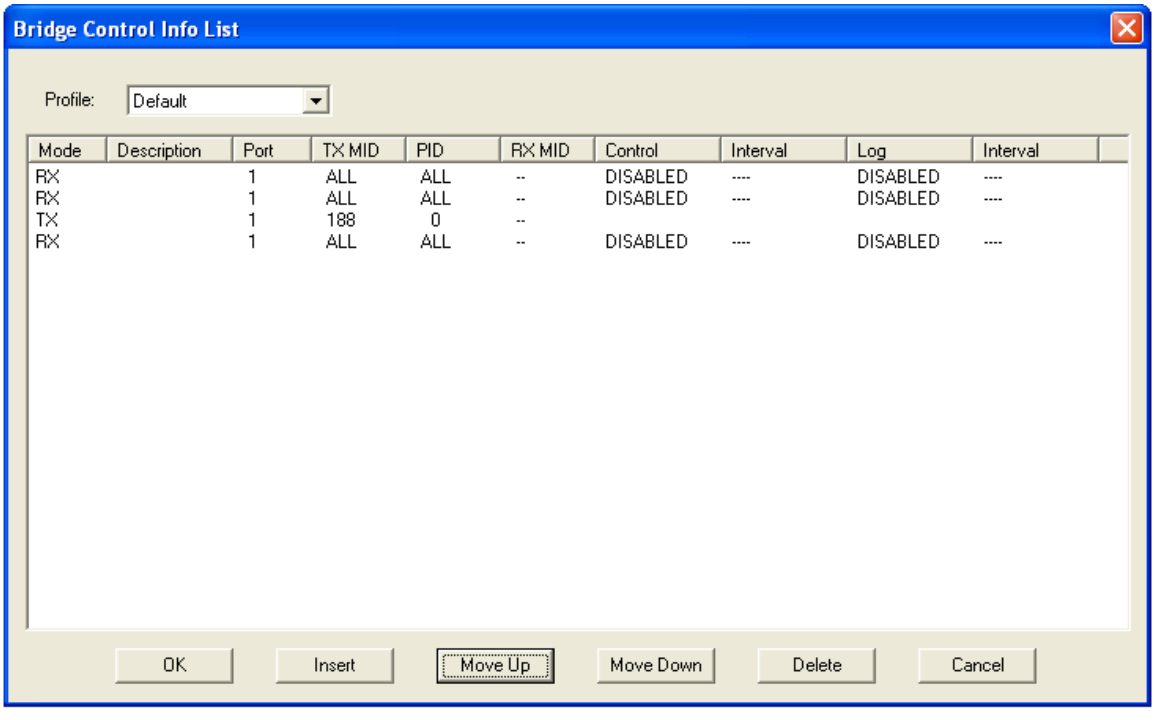


Figure 2: Populated Bridge Control Info List.

Edit Bridge Control Entry, Receive Mode

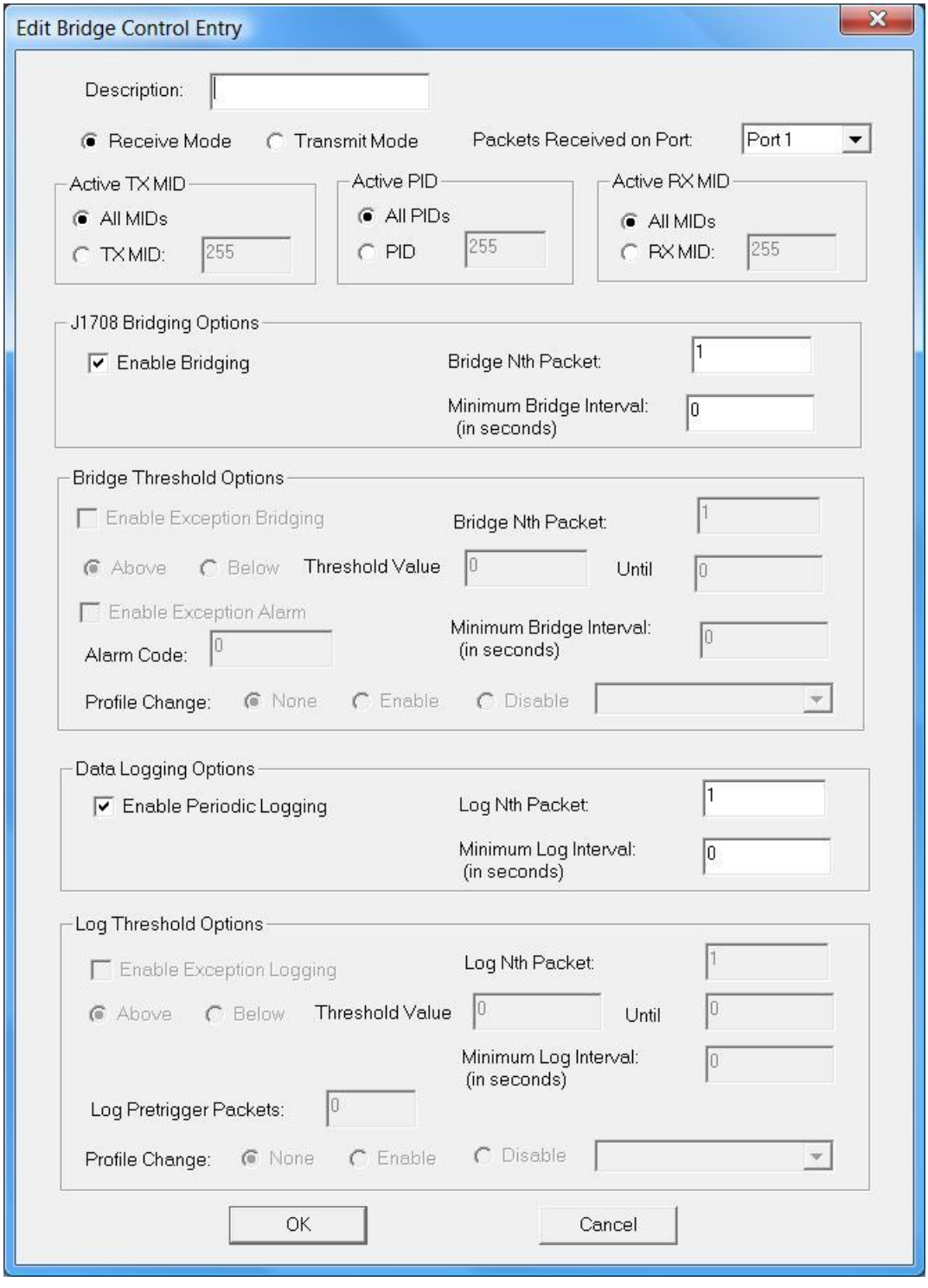


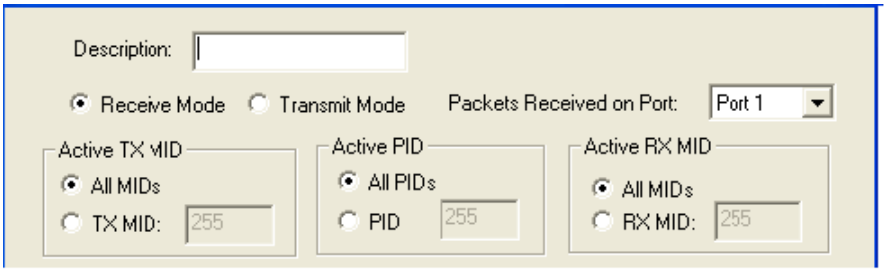
Figure 3: Edit Bridge Control Entry, Receive Mode

The following refers to the “Edit Bridge Control Entry” with "Receive Mode” selected. One can pick the J1708 packets to be bridged and logged (packet filter) by stipulating all or specific MIDs and/or PIDs.

The next sections address configuring Control Entry:

- J1708 Bridging Options
- Bridge Threshold Options
- Data Logging Options
- Log Threshold Options

While the different sections work independently, multiple sections may be enabled for the same packet filtering control.



Bridge Control Entry, Packet Filter Section

Figure 4: Bridge Control Entry, Packet Filter Section

Description:

Use this text box to describe the particular control entry.

Receive Mode / Transmit Mode Radio Button:

Determines whether this control entry controls incoming (receive) packets or outgoing (transmit) packets.

Packets Received on Port:

Select the port used for this control entry to filter packets.

Active TX MID:

Specify the Transmitter MID that the control entry will act on these packets.

Active PID:

Enter the PID that the control entry will act on these packets.

Active RX MID:

This option is valid only for PIDs 254, 510, and 511. The control entry will act on the packets with the specified receiver's MID.

Bridge Control Entry, J1708 Bridging Options

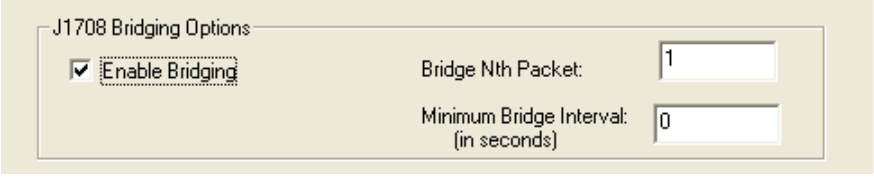


Figure 5: Bridge Control Entry, J1708 Bridging Options

Enable Bridging:

With the Enable Bridging checkbox selected, the control entry bridges J1708 packets received on the selected port to the second port (configured in packet filtering section).

Bridge Nth Packet:

Every Nth packet that matches the packet filtering criteria is bridged from the chosen receive port to the second port.

For example:

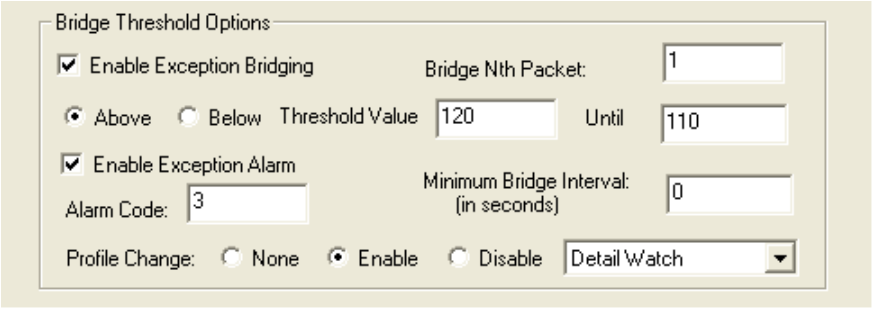
- Bridge Nth Packet = 1, each packet that matches the packet filtering conditions is bridged.
- Bridge Nth Packet = 2, every other packet that matches the packet filtering conditions is bridged.
- Bridge Nth Packet = 7, every seventh packet that matches the packet filtering conditions is bridged.

Minimum Bridge Interval:

The minimum bridge interval places timing restrictions on the Nth packet bridging.

For example:

- Minimum Bridge Interval = 0, No timing restrictions, packets are bridged based on the Bridge Nth Packet setting.
- Minimum Bridge Interval = 1, The Bridge Nth Packet setting is used if 1 second has passed since the last packet was bridged.
- Minimum Bridge Interval = 20, The Bridge Nth Packet setting is used if 20 seconds has passed since the last packet was bridged.



Bridge Control Entry, Bridge Threshold Options

Figure 6: Bridge Control Entry, Bridge Threshold Options

Enable Exception Bridging:

The enable exception bridging option allows bridging of packets based on the value of the datum contained in the J1708 packet.

Bridge Nth Packet:

Every Nth packet, which matches the packet filtering options and the threshold options, is bridged from the selected receive port to the second port.

For example:

- Bridge Nth Packet = 1, each packet that matches the packet filtering and threshold options is bridged.
- Bridge Nth Packet = 2, every other packet that matches the packet filtering and threshold options is bridged.
- Bridge Nth Packet = 5, every fifth packet that matches the packet filtering and threshold options is bridged.

Minimum Bridge Interval:

The minimum bridge interval places timing restrictions on the Nth packet bridging.

For example:

- Minimum Bridge Interval = 0, No timing restrictions, packets are bridged based on the Bridge Nth Packet setting.
- Minimum Bridge Interval = 1, The Bridge Nth Packet setting is used if 1 second has passed since the last packet was bridged.
- Minimum Bridge Interval = 20, The Bridge Nth Packet setting is used if 20 seconds has passed since the last packet was bridged.

Above/Below:

Choose whether the bridging criterion trips above or below the Threshold Value entered.

Threshold Value:

The threshold value is compared with the J1708 packet datum to execute an exception.

Until Value:

The Until value works as a hysteresis value. The threshold value generates the exception and the Until value reverses the exception.

Example: PID = 84, Threshold Value above 120

- Until Value = 120, Packets are bridged when the packet value exceeds 120 and continues bridging until the packet value drops below 120.
- Until Value = 110, The FSD J1708 bridge bridges PID 84 packets when the packet value exceeds 120 and continues bridging until the packet value drops below 110.

Enable Exception Alarm:

With Enable Exception Alarm checked, a J1708 packet, which causes an exception, will be bridged with a special alarm code added to the packet header. This feature results in a quick notification, when an exception is triggered.

An alarm packet is sent when the exception is triggered and additional alarm packets are sent if the exception value increases.

Example: PID = 84, Above Threshold value = 120, Until Value = 110

> An alarm packet is sent when the PID 84 data value hits 121. An additional alarm packet is sent each time the PID 84 data value increases. The alarm peak level is reset once the PID 84 datum reaches the Until Value, in this case 110.

If “Enabled Flash Log” is checked in the Configure Bridge Options menu, special alarm packets are also logged in the flash.

Alarm Code:

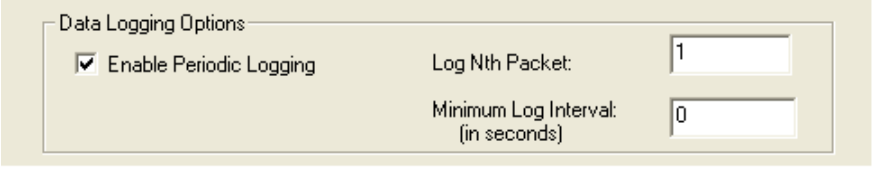
The alarm code can be set to 16 different alarm code values. (0 – 15)

Profile Change:

If multiple bridge control profiles were created, the profile change grouping allows enabling or disabling of different profiles based on exception criteria.

Thus, the user can monitor a specific variable, such as a vehicle’s road speed. If a speed exception occurs the user could enable (or disable) a different profile that specifies monitoring of other parameters such as RPM, Oil Temp, or Engine Temp.

- None – No profile action is taken
- Enable – Enable the profile listed in the profile drop list box.
- Disable – Disable the profile listed in the profile drop list box.



Bridge Control Entry, Data Logging Options

Figure 7: Bridge Control Entry, Data Logging Options

Enable Periodic Logging:

If Enable Periodic Logging is selected, this control entry logs J1708 packets received on the selected port, based on the packet filtering options specified.

Log Nth Packet:

Every Nth packet that matches the packet filtering options is logged from the selected receive port.

For example:

- Log Nth Packet = 1, each packet that matches the packet filtering options is logged.
- Log Nth Packet = 2, every other packet that matches the packet filtering options is logged.
- Log Nth Packet = 8, every eighth packet that matches the packet filtering options is logged.

Minimum Log Interval:

The minimum log interval places timing restrictions on the Nth packet logging.

For example:

- Minimum Log Interval = 0, No timing restrictions, packets are logged based on the Log Nth Packet setting.
- Minimum Log Interval = 1, The Log Nth Packet setting is used, if 1 second has passed since the last packet was logged.
- Minimum Log Interval = 20, The Log Nth Packet setting is used, if 20 seconds have passed since the last packet was logged.

Bridge Control Entry, Data Logging Options

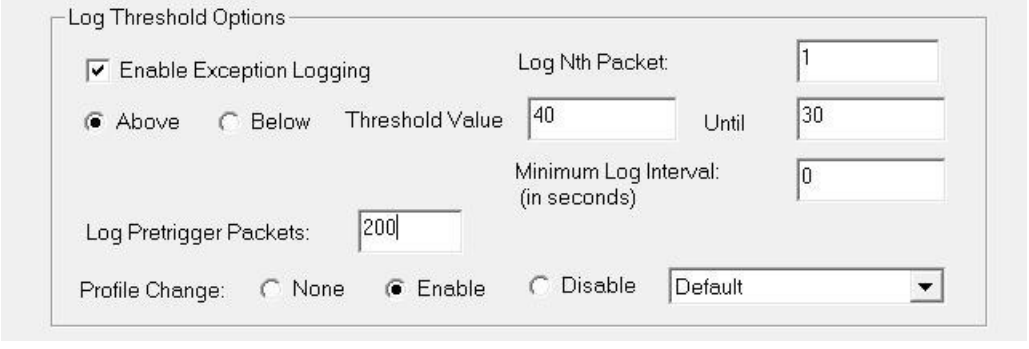


Figure 8: Bridge Control Entry, Data Logging Options

Enable Exception Logging:

The exception logging allows packets to be logged based on the datum value contained in the J1708 packet.

Log Nth Packet:

Every Nth packet that matches the packet filtering criteria and the threshold value is logged from the selected receive port.

For example:

- Log Nth Packet = 1, each packet that matches the packet filtering and threshold options is logged.
- Log Nth Packet = 2, every other packet that matches the packet filtering and threshold options is logged.
- Log Nth Packet = 9, every ninth packet that matches the packet filtering and threshold options is logged.

Minimum Log Interval:

The minimum log interval places timing restrictions on the Nth packet logging.

For example:

- Minimum Log Interval = 0, No timing restrictions, packets are logged based on the Log Nth Packet setting.
- Log Bridge Interval = 1, The Log Nth Packet setting is used if 1 second has passed since the last packet was logged.
- Minimum Log Interval = 20, The Log Nth Packet setting is used only if 20 seconds has passed since the last packet was logged.

Above/Below:

Choose whether the packet is logged when the datum is above or below the Threshold Value.

Threshold Value:

The threshold value is used to compare the J1708 packet datum to execute an exception.

Until Value:

The Until value acts as a hysteresis. When reached, the threshold value generates the exception and the Until value reverses the exception.

Example: PID = 84, Above Threshold Value = 40

- Until Value = 40, Packets are logged if the packet value exceeds 40 and packets continually logged until the packet value drops below 40.
- Until Value = 30, The FSD J1708 bridge begins logging PID 84 packets once the packet data value exceeds 40 and continues to log PID 84 packets until the packet data value drops below 30.

Log Pretrigger Packets:

Enter a value from 0 to 200, which indicate the number of packets that are logged just prior to the trigger.

Profile Change:

If multiple bridge control profiles were created, the profile change grouping allows enabling or disabling of different profiles based on exception criteria.

Thus, the user can monitor a specific variable, such as a vehicle's road speed. If a speed exception occurs the user could enable (or disable) a different profile that specifies monitoring of other parameters such as RPM, Oil Temp, or Engine Temp.

- None – No profile action is taken
- Enable – Enable the profile listed in the profile drop list box.
- Disable – Disable the profile listed in the profile drop list box.

Edit Bridge Control Entry, Transmit Mode

When “Transmit Mode” is selected in the Edit Bridge Control Entry dialog box, the Edit Transmit Control Entry dialog is displayed. (Figure 9)

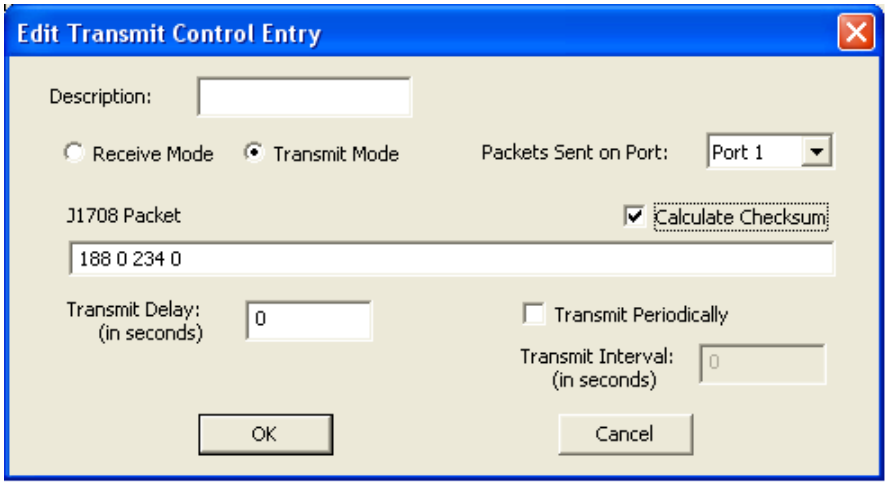


Figure 9: Edit Bridge Control Entry, Transmit Mode

If you need to monitor packets that are not typically broadcast, the Transmit Control Entry allows users to define transmit packets such as PID 0 request packets.

Description:

Enter text box to describe the particular control entry.

Receive Mode / Transmit Mode Radio Button:

The user selects the radio button to designate this control entry to control either incoming (receive) packets or outgoing (transmit) packets. Selecting Receive Mode reverts to the “Edit Bridge Control Entry” dialog (Fig. 3).

Packets Sent on Port:

Select the port used to transmit the J1708 packet.

J1708 Packet:

Enter the J1708 packet, in decimal format.

Calculate Checksum:

Select the calculate checksum, if you want the control entry to calculate the J1708 packet checksum automatically. Insert a placeholder value at the end of the packet for the checksum.

Transmit Interval: Valid Range: (0 – 65535). If Transmit Periodically is enabled, the entered value dictates how often the packet is transmitted.

Transmit Delay:

Valid Range: (0 – 65535).

The transmit delay specifies the time period before transmitting the packet, after the controller powers up or profile is enabled.

Transmit Periodically:

Select transmit periodically to send the packet every “Transmit Interval” after the transmit delay time has passed.

FSD J1708 User Reference Guides

Select the FSD J1708 topic below to display its reference information.

J1587 Decoding Options

J1708 Simulation and Automated Test Script – Describes how to use a script with J1708 packets to simulate J1708 conversations and to automate testing.

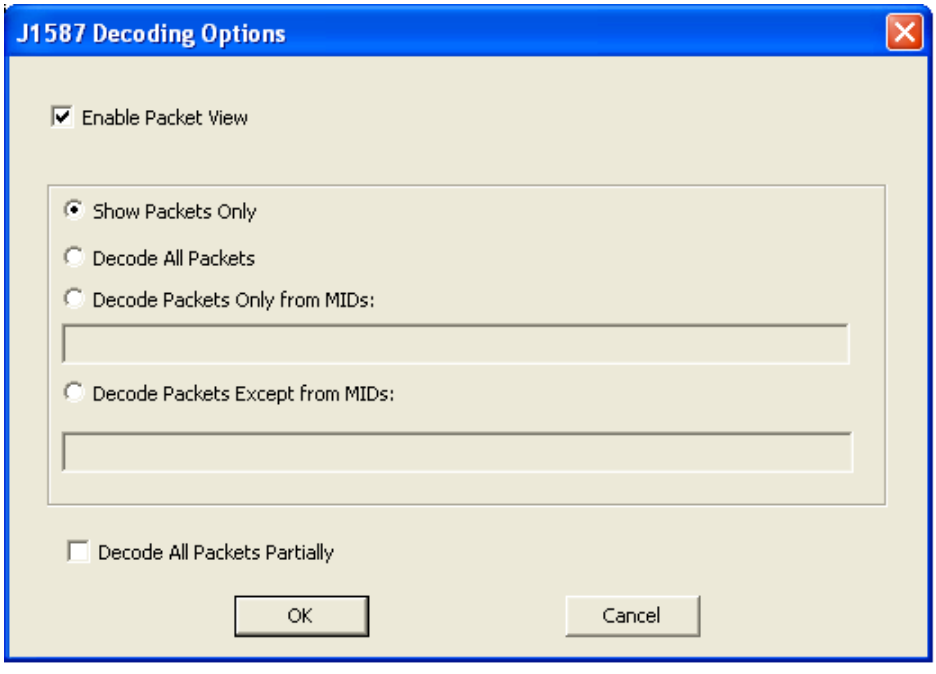
Example J1708 Bridge Configuration

FSD Remote Access Configuration Guide - Describes steps to configure controller for remote access.

FSD SEND_J1708 Utility Usage Notes

FSD Third Party Application_Interface Guide

J1587 Decoding Options



Enable Packet View:

Selecting the packet view displays all decoding to the screen.

Show Packets Only:

Packet values are shown to the screen, without decoding of the packets.

Decode All Packets:

Fully decode all packets to the screen.

Decode Packets Only from MIDs:

All packets are displayed, but only packets from the listed MIDs are decoded.
Example List: “128 188 187”

Decode Packets Except from MIDs:

All packets are displayed and decoded except packets with the listed MIDs.
Example List: “128 188 187”

J1708 Simulation and Automated Test Script Commands

Overview

Many J1708/J1587 simulation scripts are linear sequences of J1708 packets to send. With these scripts, J1708 Tester provides some control over which packets in the script to send, packet transmission timing, repeating the script continuously, and so forth. This capability is often sufficient to provide a good engineering design and test environment for developing J1708 devices. It provides a good way to do both one-time testing, where an engineer is closely watching the packets and responses, and to repeat problematic packet sequences to debug the device software.

Additional script file capabilities provide support to automate repetitive test activities, which might be needed in a manufacturing test environment.

Script commands can interact with the user, control the flow of the scripts, and insert comment lines into the generated output window text and log file. These script commands implement a simple interpreted programming language that provides a fair amount of capability without developing a custom C++ application. For example, by adding a few text lines to a script, you can have the script send a sequence of J1708 packets, then display a message box asking whether a desired condition was observed; and depending on whether the user clicks the YES or NO button, either continue to the next stage of a test or repeat the sequence.

The FSD J1708 Tester script commands also allows integration of other analog and digital inputs and outputs into the J1708 packet based test setup. Script commands let you set the output states of devices such as relays, voltage levels, or 4-20 ma current levels, and read measured input values from devices including switches, any 4-20 ma sensors, and other input devices. The input states can be used to control script execution. For example, a script can send a sequence of J1708 packets, read a relay contact state or pressure sensor value, and if the value is out of the expected range, display a message box to alert the test operator that a test condition has failed.

Note that to read and control the non-J1708 input/output devices requires control ability not found in the J1708 Tester controller. FSD offers another controller model, the FSD Bridge Controller Plus, an associated device family that can be used for this purpose and is directly supported by the J1708 Tester script commands. The script language also can support any other third-party I/O control devices used, as long as one writes interface software, if needed.

Sample Script and Capture Log Files

Sample simulation script files and capture log files are provided in the <installation root>\samples folder.

Sample Script Files:

To run the sample script files, move the "xxx.jt_scr" files to the <installation root>\data folder, then from the J1708 Tester menu select Simulation → Set Script Options and select a script from the dialog. Next from the Simulation menu choose Enable Script, then Enable Simulation. View sample script files with any text editor, and selected J1708 packet definitions can be cut-and-pasted from these script files into other script files, the user-defined packets dialog, or repetitive packet dialog, then modified as desired.

Sample script files include:

test_pids.jt_scr -- sample J1708 packets for most PIDS

test_script_commands.jt_scr – demonstrates the usage of many of the script language control flow and non-J1708 device input and output control features.

Sample Capture Log Files:

The sample log files show J1708 packet data captured from a Freightliner truck. These log files were captured and distributed in binary log form, in file named "xxx.jt_blog". To use them copy them to your DATA folder, and under the Logging menu select "Extract Log" and enter your desired decoding options. This generates a text log output file, "xxx.jt_log". Rename or copy the text log file to "xxx.jt_scr" for use as a script file. You may edit this file with a text editor. You may also cut-and-paste packets from this file into the "Test User Defined Packets" screen.

Sample capture log files include:

Freightliner_1.jt_blog
Freightliner_2.jt_blog
Freightliner_3.jt_blog
Freightliner_4.jt_blog

If you have the opportunity to capture a binary log file from a different make/model vehicle and are willing to share it, we would appreciate the opportunity to add it to our sample capture file collection. (For capturing high density packet streams from live vehicles, we recommend turning off packet viewing in the "View J1587 Decoding Options" screen, since writing the decoded packets to the screen can slow down the computer and reduce responsiveness to user commands, particularly with LCD laptop screens.)

Script Command Reference

Script Comments

";" comments within the script file used for script file documentation are preceded by a semicolon.

Note that J1708 packet information captured from J1708 Tester's view window or copied from its packet log can be directly used within a script file. Decoded J1708 packet parameter information are preceded with comment semicolons.

J1708 Transmit Packets:

--> [days-hour:minute:seconds.milliseconds] 123 456 789 012 …

J1708 Receive Packets:

<-- [days-hour:minute:seconds.milliseconds] 123 456 789 012 …

--LONG_TX_PKT
(TBD)

--LONG_RX_PKT
(TBD)

User Interaction and Timing Commands

--COMMENT <text line>

The COMMENT script command places the entered text line in the view window and in the log file, if text-mode logging is enabled.

--SLEEP <sleep time in milliseconds>

The SLEEP script command pauses script execution for the entered number of milliseconds, then the script continues without user interaction.

--PAUSE <text line>

The PAUSE script command displays a message box containing the supplied text line, and pauses simulation until the user selects OK to continue or CANCEL to end the simulation. The PAUSE command also places the text line in the view window and in the log file, if text-mode logging is enabled.

--PAUSE_YES_NO <text line>

The PAUSE_YES_NO script command displays a message box containing the supplied text line, and pauses simulation until the user selects YES to return a TRUE value, NO to return a FALSE value, or CANCEL to end the simulation. The returned truth value can be used by IF_TRUE, IF_FALSE, JUMP_TRUE, and JUMP_FALSE commands to affect the script execution sequence. The PAUSE_YES_NO command also places the text line in the view window and in the log file, if text-mode logging is enabled.

Software Interaction Commands

--SEND_DE <SET | QUERY> <device identification and element parameters> <query results file name> <APPEND option>

The SEND_DE script command controls and reads device input and output states. For example, use it to control a relay or motor, read a switch position, read a counter or pulse rate value, or read a 4-20 milliamp analog measurement value. The SET option sets a state, and the QUERY option reads a state value. QUERY results are placed in a text file.

SEND_DE works in cooperation with separate FSD automation controller and automation software suite. Detailed documentation of the SEND_DE parameters is provided with the automation software suite, along with discussions of other related device control topics.

SEND_DE looks for the separate FSD automation controller software specified in the "Automation" folder path under the Options menu -> "Set J1708 Tester Options".

--SEND_DE_2 <SET | QUERY> <device identification and element parameters> <query results file name> <APPEND option>

The SEND_DE_2 script command allows use of an additional automation controller or emulation controller. SEND_DE_2 behaves the same as the SEND_DE command, except that it looks for the additional FSD automation controller software under the "Emulation" folder path specified using "Set J1708 Tester Options".

--READ_DE <query results file name>

The READ_DE script command reads the SEND_DE query results file, merging the query results report with the J1708 packets on the J1708 Tester's view window. The READ_DE command also places the query results in the log file, if text-mode logging is enabled.

READ_DE also reads a TRUE/FALSE value of the SEND_DE query results, and an INTEGER value of the query results, which can be used by the Execution Control script commands to implement conditional execution of the simulation script.

READ_DE looks for the SEND_DE results file under the “Automation” folder path specified using “Set J1708 Tester Options”.

--READ_DE_2 <query results file name>

The READ_DE_2 script command reads the SEND_DE_2 query results file. READ_DE_2 behaves the same a the READ_DE command, except that it looks for the SEND_DE_2 results file under the “Emulation” folder path specified using “Set J1708 Tester Options”.

--RUN

The RUN script command invokes the execution of any other program during the J1708 simulation. This may be used as one wishes. If the executed program generates a text file, the READ_DE command can be used to place the results in the J1708 Tester view window and in a text-mode simulation log file.

--SET_TRUE
Sets the active truth value to TRUE.

--SET_FALSE
Sets the active truth value to FALSE.

--SET_VALUE <integer value>
Sets the active integer value to the supplied <integer value>. The active integer value can be used in value comparison commands such as IF_EQUAL and JUMP_GREATER_THAN to determine the script command execution sequence.

--COPY_VALUE_TO <variable_name>
Copies the active integer value to a variable named <variable_name>. Up to 16 named variables can be used in a simulation script.

--COPY_VALUE_FROM <variable_name>
Copies the integer value of the variable named <variable_name> to the active integer value.

--SHOW_ACTIVE_VALUES
Shows the active integer and truth values.

--SHOW_STORED_VALUES
Shows the stored values of all the named variables.

--INCREMENT
Increments the active integer value.

--DECREMENT
Decrements the active integer value.

Conditional Execution Commands

--IF_TRUE

The IF_TRUE script command conditionally executes a block of script commands depending on a SEND_DE query result value. If the result value is FALSE, script execution skips to the matching ELSE or ENDIF script command.

Nested IF-ELSE-ENDIF script commands are supported.

--IF_FALSE

The IF_FALSE script command skips to the matching ELSE or ENDIF script command if the result value is TRUE.

--IF_EQUAL <integer_value>
--IF_NOT_EQUAL <integer_value>
--IF_LESS_THAN <integer_value>
--IF_LESS_THAN_OR_EQUAL <integer_value>
--IF_GREATER_THAN <integer_value>
--IF_GREATER_THAN_OR_EQUAL <integer_value>
The IF_(value comparison) script command skips to the matching ELSE or ENDIF script command if the comparison of the active integer value to the specified <integer_value> is TRUE.

--ELSE

The ELSE script command is an optional skip-to destination for the IF_TRUE and IF_FALSE commands. If the preceding IF_ command does not skip to the ELSE command, then the ELSE command skips to the matching ENDIF command.

--ENDIF

The ENDIF script command is a skip-to destination for the IF_TRUE, IF_FALSE, and ELSE script commands.

Jump and Conditional Jump Commands

--LABEL <label>
Labels a script command line with the name <label>, which can be used to target any type of JUMP command

--JUMP <label>
Unconditional jump to the specified label

--JUMP_TRUE <label>
Jumps to the specified label if the active truth value is TRUE.

--JUMP_FALSE <label>
Jumps to the specified label if the active truth value is FALSE.

--JUMP_EQUAL <label> <integer_value>
--JUMP_NOT_EQUAL <label> <integer_value>
--JUMP_LESS_THAN <label> <integer_value>
--JUMP_LESS_THAN_OR_EQUAL <label> <integer_value>
--JUMP_GREATER_THAN <label> <integer_value>
--JUMP_GREATER_THAN_OR_EQUAL <label> <integer_value>
Jumps to the specified label if the comparison of the active integer value to the specified <integer value> is TRUE.

Function Commands

--FUNCTION <function_name>
Assigns the name <function_name> to the entry point script command line of a function, which is used as the target of a CALL command.

--CALL <function_name>
Transfers script command execution to the function <function_name>, also saving the current script command line for use with the function RETURN.
Function calls may be nested up to four deep.

--RETURN
Returns from a function call, transferring script execution control to the script command line saved by the corresponding CALL to the function.

--END_SIMULATION

The END_SIMULATION script command terminates the J1708 simulation. This command is typically used within an IF-ELSE-ENDIF construction for conditional script termination. For example, the END_SIMULATION might be used to stop an automated test session, if an error condition is detected.

Example J1708 Bridge Configuration

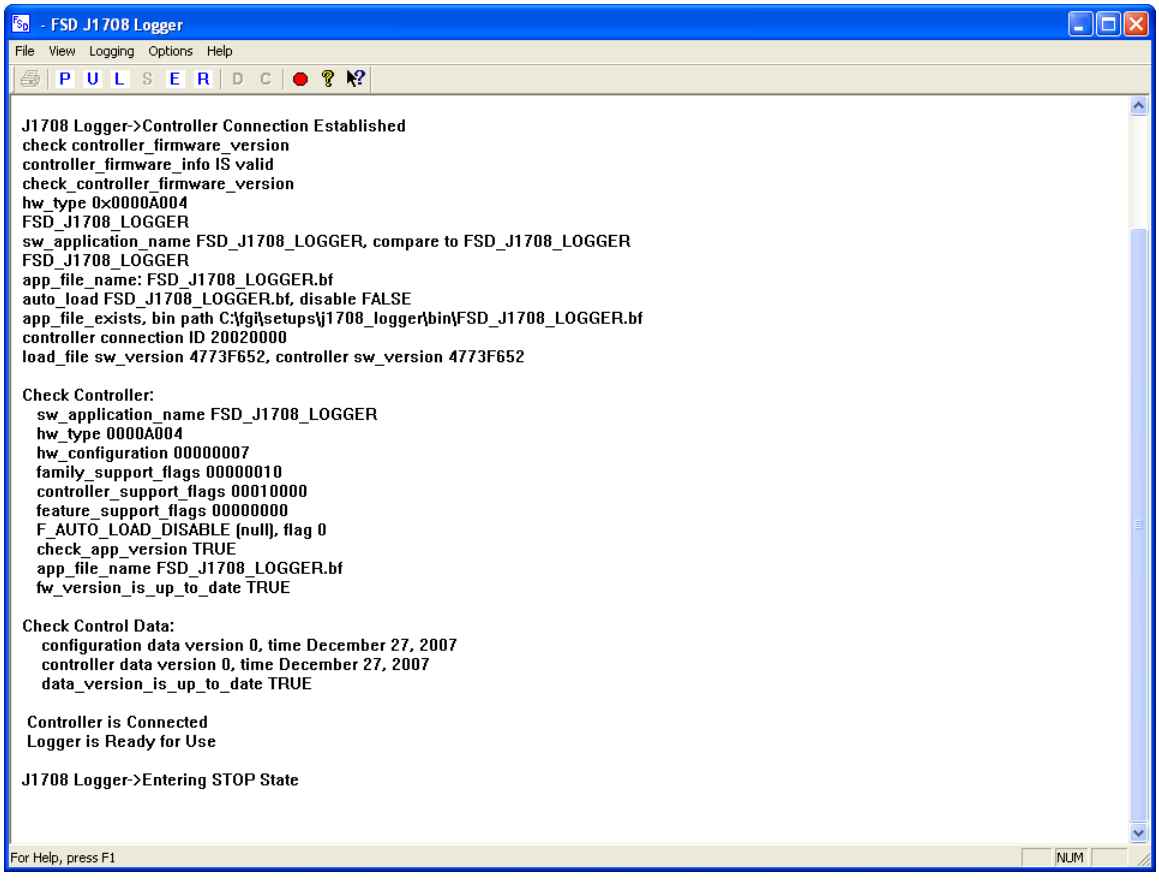
This document explains the configuration of a J1708 Bridge device for Bridging or Logging (if equipped for logging). This explanation assumes a completed software installation and the computer serial port is connected to the FSD J1708 Bridge.

This example illustrates how to:

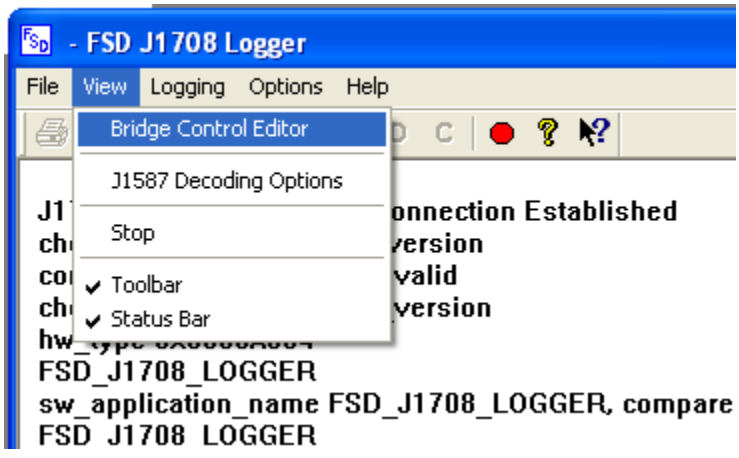
- Bridge all PID 190 packets.
- Bridge all PID 84 packets if the data in the packet exceeds 40

1. Begin by starting router.exe. \<your_install_directory>\bin\router.exe
2. Start j1708_logger.exe. \<your_install_directory>\bin\j1708_logger.exe

The J1708_logger screen appears.

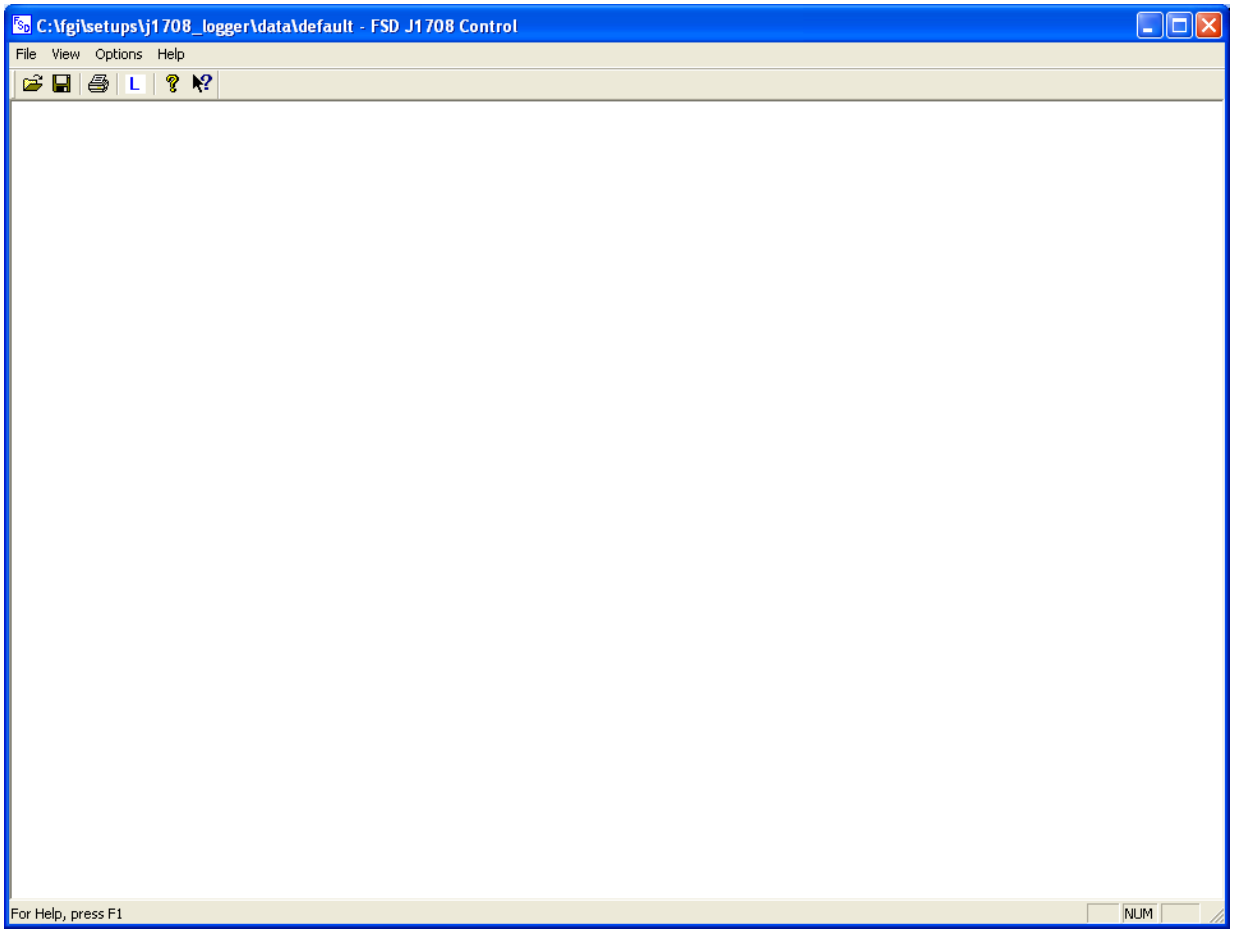


Start the FSD J1708 Control editing program:



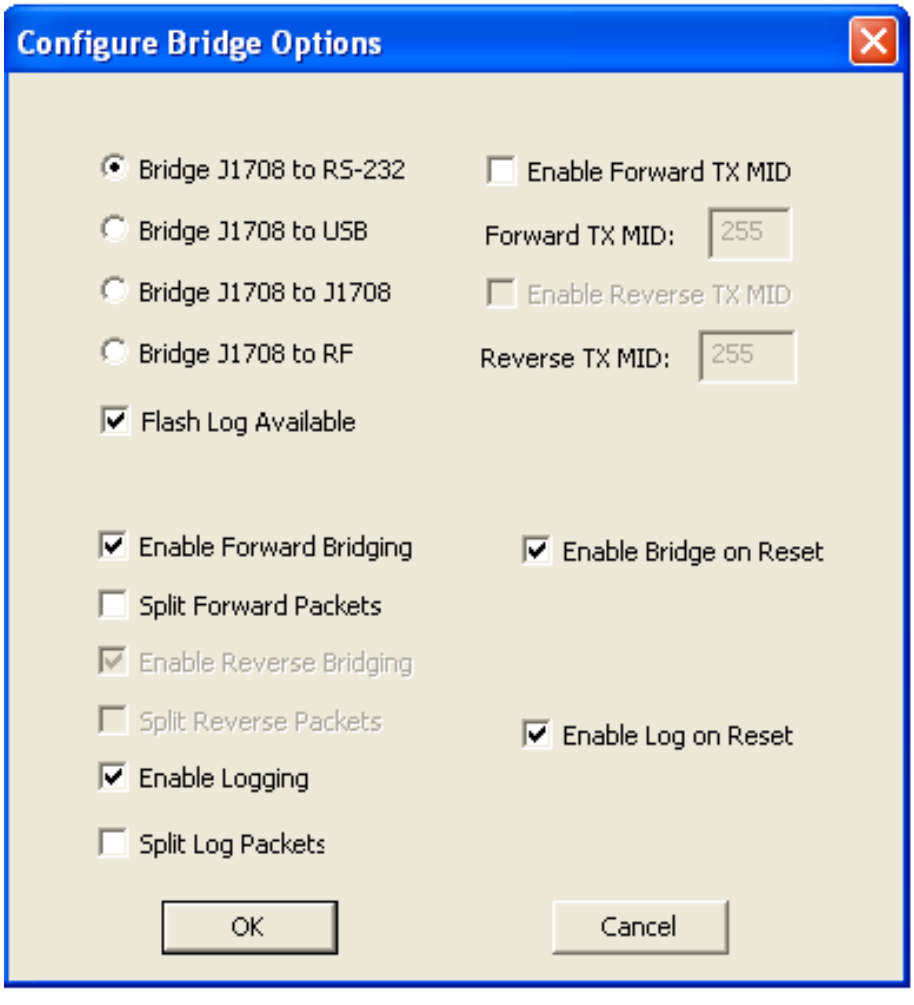
From the menu select View->Bridge Control Editor to start the FSD J1708 Control program to edit the bridge control list.

The following screen appears.


C:\fgi\setups\j1708_logger\data\default - FSD J1708 Control
File View Options Help
For Help, press F1
NUM

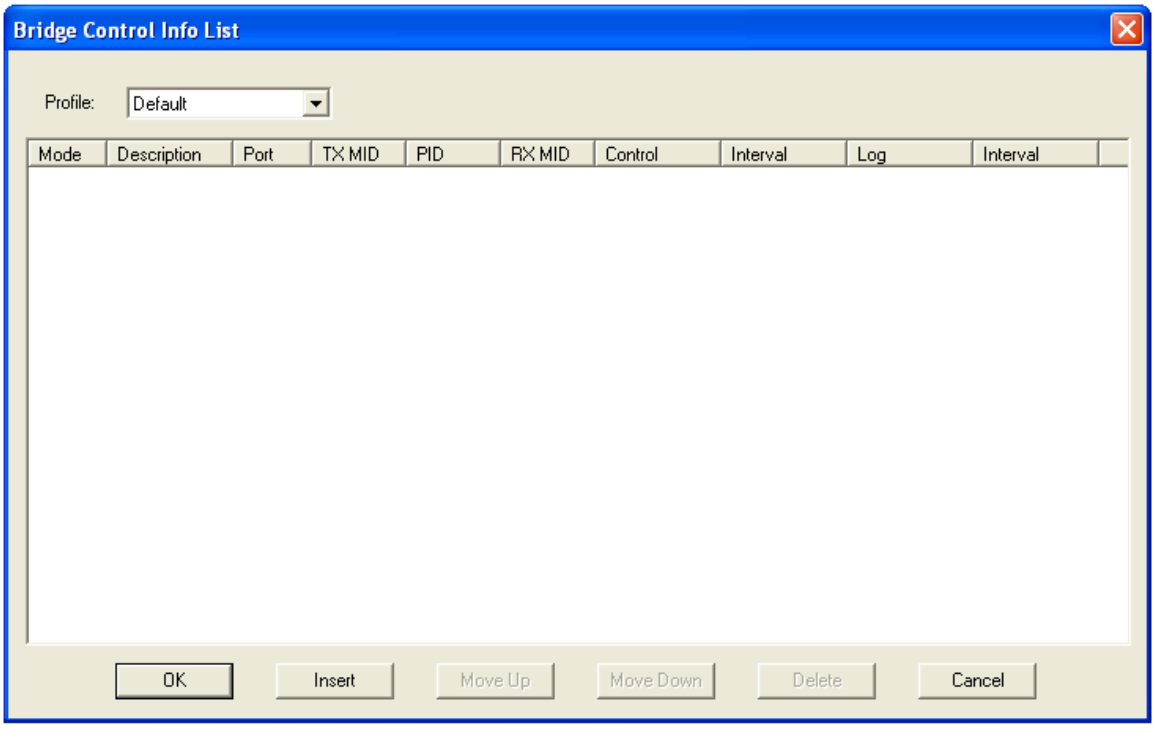
Configure the global control options:

From the menu select Options->Configure Bridge Options, and from the dialog displayed select the appropriate options for the hardware that is being configured from the following dialog. (For detailed explanation on settings see the J1708 Control User Guide.) Click “OK” to set configuration.

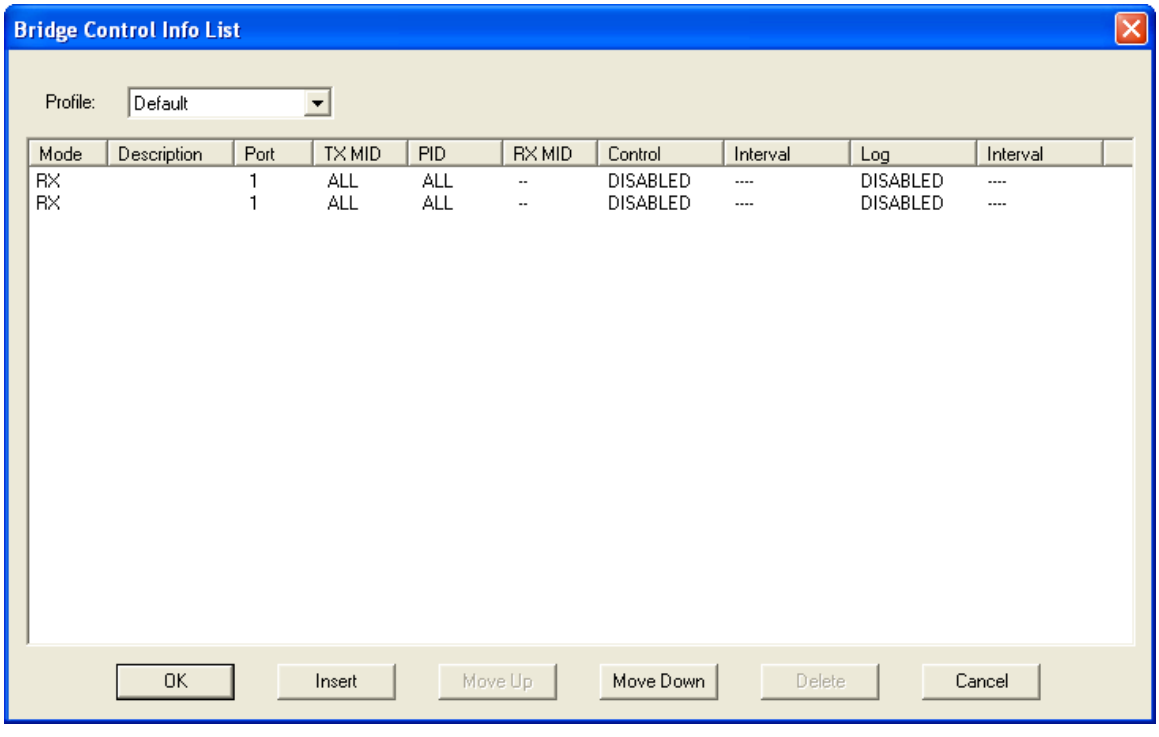


Configure the Control Parameters:

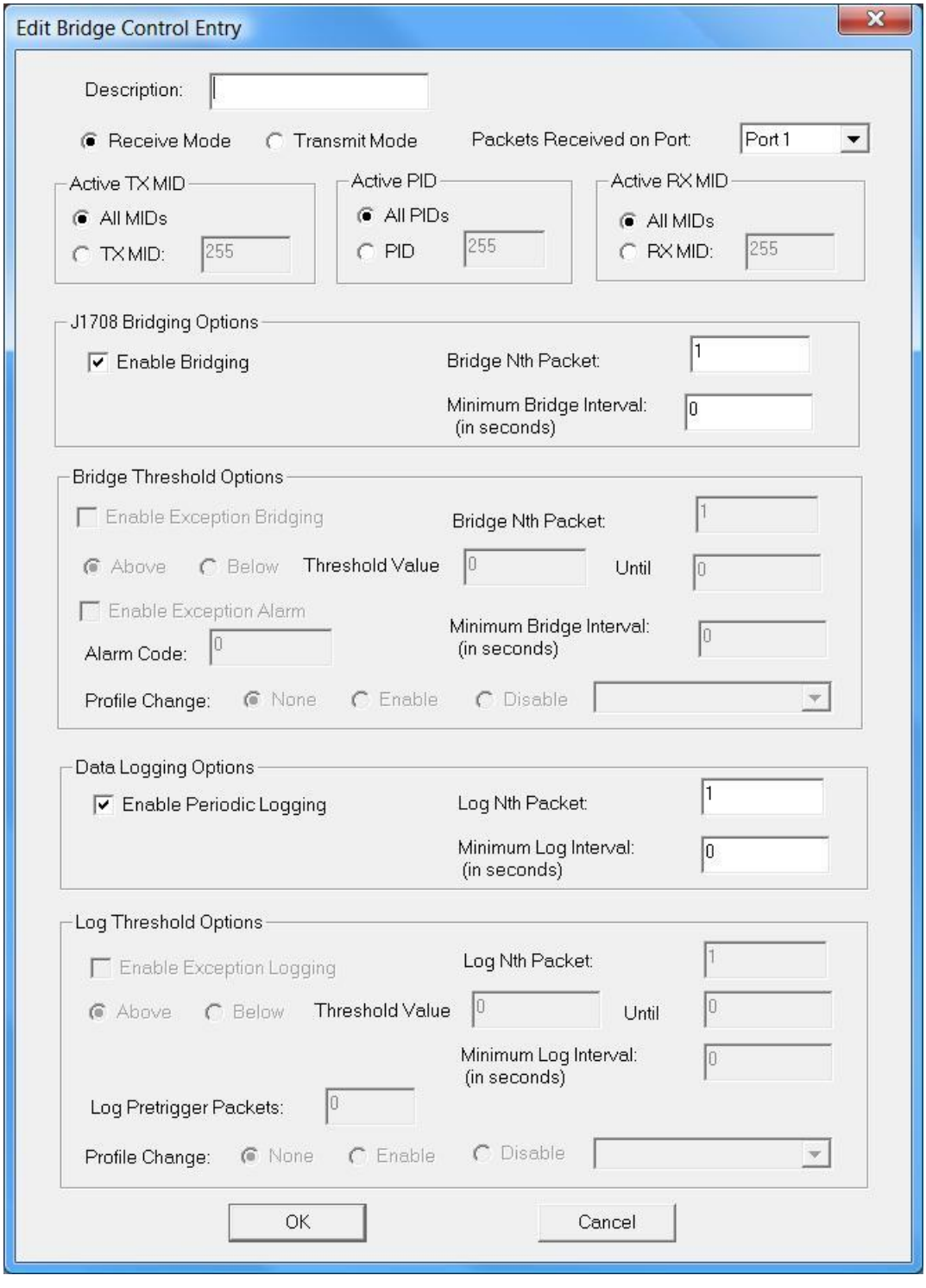
From the menu select Options->Configure Bridge Control to display the Bridge Control Info List dialog box.



Click Insert to add blank control entries to the Control Info List.



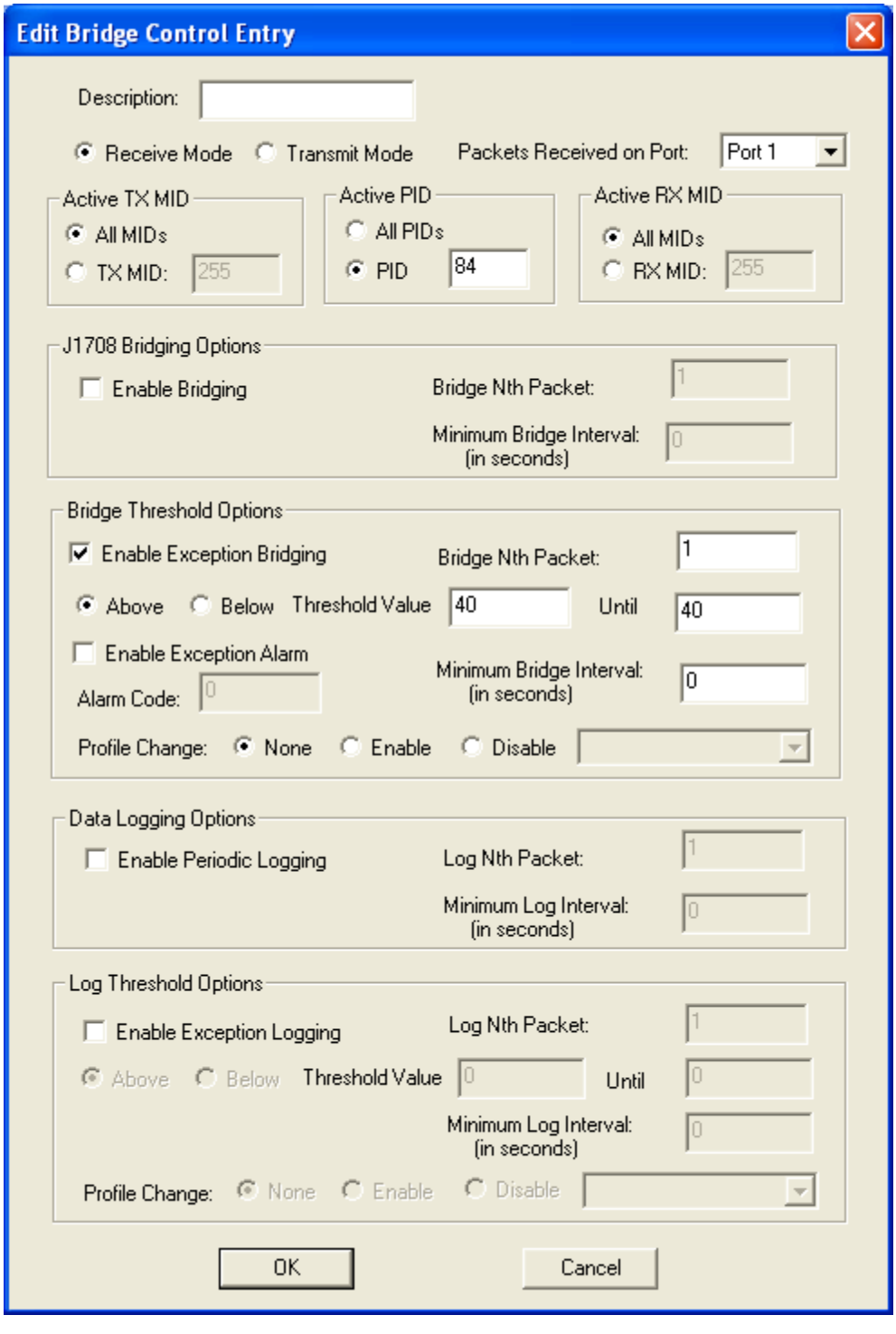
Double click on the first line item and edit the entry dialog for the first bridging criterion “Bridge all PID 190 packets”.



Under the Active PID, select PID and enter 190. Select the Enable Bridging in the J1708 bridging Options section. (For detailed explanation on settings see the J1708 Control User Guide.)

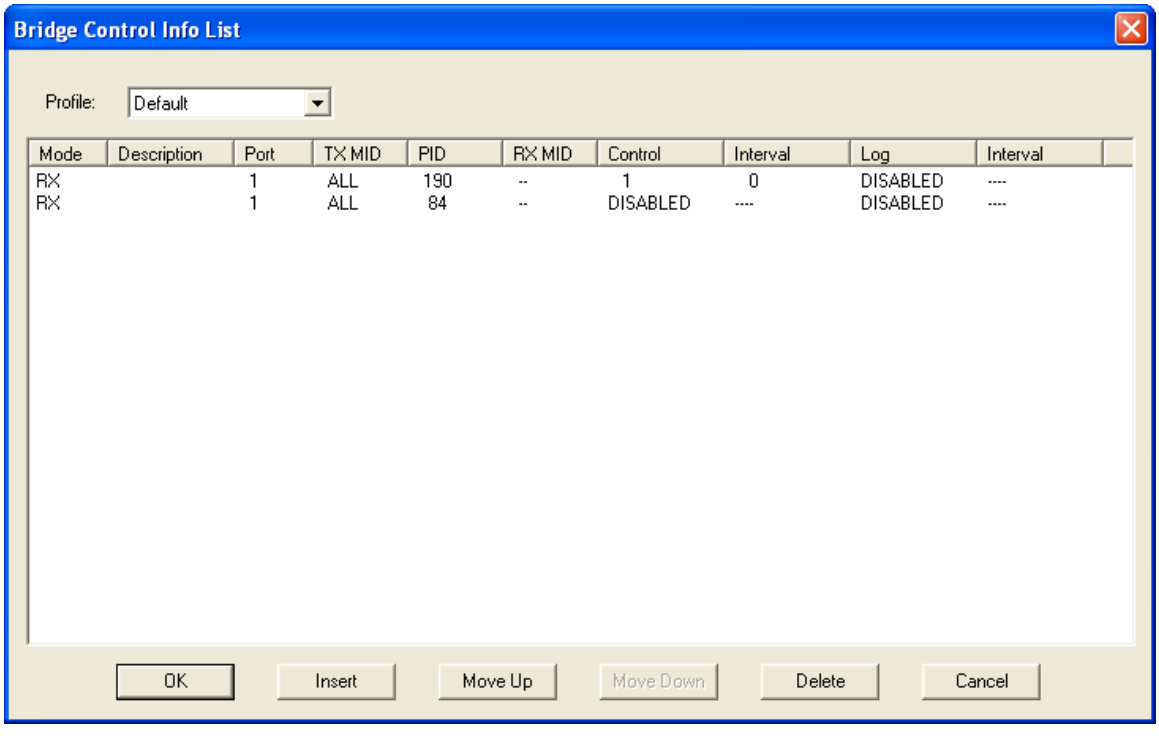
Click OK.

Double click on the second line item in the Bridge Control Info List and Edit the dialog box for the second bridging criterion “Bridge all PID 84 packets if the data in the packet exceeds 40”. Choose the “Above” radio button and enter the value “40” for threshold value.

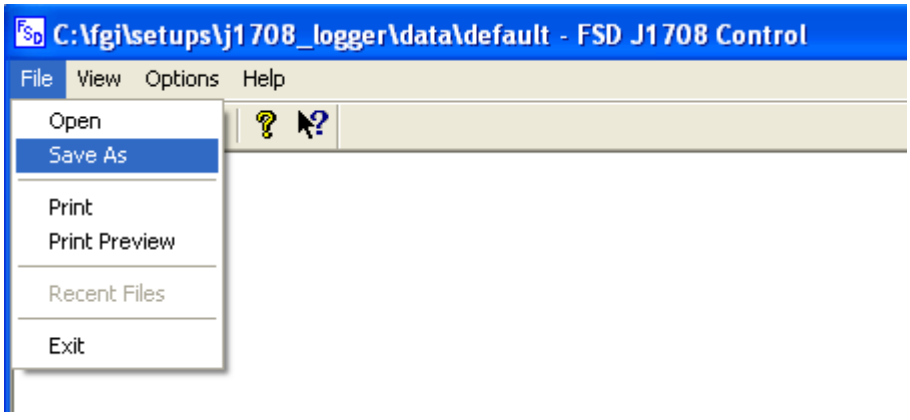


Under Active PID, select PID and enter 84. Select the Enable Exception Bridging options in the Bridge Threshold Options. Enter 40 for the Threshold Value and the Until Value. The Bridge begins bridging PID 84 packets when the data goes above 40 and continues bridging until the data drops below 40.

Click OK. The Bridge Control Info List has now been populated to meet the bridging criteria initially specified.



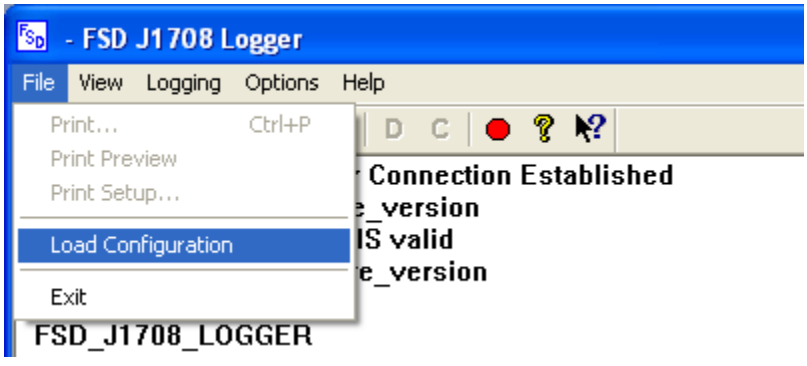
Click OK. A J1708 bridge configuration file has been created in "\<your_install_directory>\data\default.jt_bcfg". Select "Save As" under the File menu to save the file with another name.



The J1708 bridge control entry is now complete and the program may be closed to return to the J1708 Logger program.

Load Configuration file to the Bridge:

In the J1708 Logger program, from the menu select File->Load Configuration to load the configuration to the FSD J1708 Bridge device.



FSD Remote Access Configuration Guide

FSD controller software, and third party custom software, can access FSD controllers via a LAN, Wireless LAN, or the Internet using the TCP/IP protocol.
The programming model used for remote access is based on having the FSD software running on a host computer connected directly to the FSD controller, and also installed on each additional computer accessing the system remotely. Components of the host based FSD software route packets between the remote computers and the FSD controller,
and also synchronize configuration data among the computers. This approach provides close to full functionality for high performance remote monitoring, control, and configuration of the system.
By contrast, a browser based approach might typically provide a more limited, lower performance solution, with the advantage of not requiring FSD software to be installed on the remote computers.
The host computer must be a Windows XP (any variation) or Windows 2000 machine connected to the LAN or Internet, but does not need to be a LAN server or to run Internet server software. For Internet access, a high speed always-on connection is desirable so the controller may be dependably accessed while away, but the software can work with standard dial-up service. A static IP address is nice but not required; the FSD software includes a feature for automatically finding connection addresses via an Internet based directory service.
Configuring remote access involves a number of steps at the host computer and the remote client computer.
Warning: Optimally configuring a system for remote access may require
Host Computer Configuration:
1) If running in floor plan Viewer mode, select “View FSD Automator” from Viewer’s system menu (accessed by clicking the icon on the left end of Viewer’s title bar).
2) From the Automator menu, select Options _ Configure Router Options
3) Router will become visible, with an active dialog box for selecting serial port options. Click on the CANCEL button to close the dialog box.
4) From the Router menu, select Options _ Select Access Options
5) Select desired access privilege levels for LAN and Intenet access, enable appropriate password requirements, and set passwords. Passwords set at the Router level are used by
all enabled access levels for LAN and Internet access.
6) Close Router, then restart Automator (using Autostart); make Automator visible as in step 1 above if needed.
7) If the host computer has an always-on connection to the Internet: From the Automator menu, select Options _ Select Autostart Options, and enable “Start Router as a Service”. With this selection, Router will be automatically started whenever the computer reboots, so the controller can be accessed remotely without having to first log on to the host computer and manually start Automator.
8) Note that when configured for remote access, some invisible components of the FSD Automator software system will continue to run after Automator is closed with a normal exit, so that the system may still be accessed remotely. To shut down all components of

the system, from the Automator menu select File _ Shutdown Server.
9) Note that if Router has been started as a service as in step 7 above, it cannot be accessed from the Automator menu as in step 2 above. To change remote access options,
shutdown the server as in step 8 above, then restart Automator (using Autostart). Then with Automator visible, proceed with Options _ Configure Router Options.
10) If directory lookup services will be used for finding TCP/IP addresses, to prepare for configuring the remote computers the FSD controller “name_id” must be found. One way to find this is from the Automator menu select
Options _ Configure Automator Options and observer the Controller Name ID field. Alternatively, select View _ Lister _ FGI Devices, find the controller in the device listing, and copy down the “name_id” from the displayed information.
11) Note that for remote access, any firewall services on the host computer and possibly on one’s Internet router will need to have Router and Syserver access unblocked. By default, FSD Router is set to use TCP/IP port 7100, and FSD Syserver is set to use TCP/IP port 7110; these port numbers can be changed from the Router menu Options _ Configure Router Options.
12) Note that if a Host computer is to be configured to allow access to more than one connected FSD controller, additional measures must be taken. Do a Check for Updates from Automator Options or the Viewer system menu, and then view this guide from the installation root\manuals directory for additional instructions, or contact FSD for further instructions.
Remote Access Computer Configuration:
1) Start the FSD software with Autostart; if needed make Automator visible as above. The software can be expected to fail to find a Router connection.
2) From Automator, select Options _ Configure Automator Options.
3) For using directory services, enter the FSD controller “name_id”, and select “find address automatically”. Both the host computer and the remote client computer must have Internet access for directory services to work.
4) Alternatively, static LAN and/or Internet addresses may be manually entered, and the appropriate access type enabled.
5) Close the dialog and restart the application.
6) If the remote client computer has a firewall installed that blocks outgoing accesses, configure the firewall to allow communications as in step 11 of the Host computer setup instructions.
7) Note that if a remote client computer is to be configured to access more than one FSD controller, the software should be installed with a separate installation root directory for each controller accessed.

SEND_J1708 Utility Usage Notes

The SEND_J1708.EXE application is a utility for sending J1708 Packets to the FSD J1708 Tester from the command line or a third party application.

Instructions for use from the command line:

1) FSD Router must be running connected to the controller.
2) From the c:\fsd\j1708_tester\bin folder, execute SEND_J1708.EXE with command line parameters as discussed below.
3) On the command line type:

   Send_j1708 SEND "188 0 194 130" TRUE
4) The first parameter is always SEND
5) The second parameter is quoted string of J1708 packet bytes, content of each byte in decimal as is normal in J1708 documentation. Last byte is the J1708 checksum
6) The third parameter – if TRUE, the utility will calculate the J1708 checksum for you and replace the last byte in your supplied packet with the correct checksum. You DO need to supply any checksum value as a placeholder byte, it could always be '0' for example. If FALSE, the packet will be send as supplied with no checksum calculation applied.
7) The SEND_J1708 utility can be launched from within a batch file, or from a desktop icon, if desired.

Instructions for use in a third-party application program:

1) FSD Router must be running, connected to the FSD J1708 Tester, or the third party program should spawn Router. FSD Router can be configured to run invisibly in the background as a service if desired, running automatically whenever the computer is turned on.

2) The third party program (command line or Windows program) can spawn SEND_J1708 with the desired J1708 packet data to be sent using the C runtime library "spawn" family of functions, or from standard Windows methods for spawning processes.

3) This utility communicates with FSD Router via TCP-IP, so can be run remotely via a network or WiFi if that is useful to you (FSD Router must be configured to allow remote access).

FSD Third Party Application Interface

The FSD automation controllers and software system are designed to facilitate third party and custom application integration. FSD provides these applications with a means to receive sensor data from and send device control data to the automation controller and its controller devices via USB, RS-232, and standard TCP/IP packets, so the custom applications can easily interface with the real world from the local host computer, across a network, and/or via the Internet.

When interfacing with the FSD automation system via TCP/IP, the custom application first establishes a connection with the FSD Router, and then proceeds with a packet conversation with the FSD Automation Controller. When using USB or RS-232 communication, the third party applications communicates directly with the FSD controller via the computer's COM port, without using the FSD Router TCP/IP to COM port bridge program.

USB communication is accomplished via a virtual COM port installed as part of the USB driver. For use with Router, the assigned COM port should be in the range of COM1-COM9, if a different assignment is shown in Device Manager use the port's Properties/Port Settings/Advanced to manually reassign the COM port. Note that reusing a port shown as "In Use" is OK as long as the device previously assigned the port value is not simultaneously connected to the computer.

Custom Application to FSD Router Conversation:

On Custom Application Start-Up:

1) Establish a TCP/IP socket connection with FSD Router, port ID as set on the FSD Router options dialog (the default port used is 7100).

2) FSD Router will then control the packet conversation until the connection permissions are established, including a password exchange if FSD Router is configured to require a password for system access.

In the packet protocol, participating applications use packet source and destination connection IDs to control packet routing to the appropriate recipients. Custom applications should base their application connection IDs on the value:

#define CUSTOM_APPLICATION_BASE_ID 0x22F00000

Commercial third party applications may use other base IDs assigned by FSD.

Additionally, applications may send and receive broadcast packets addressed to all interested recipients, where the destination connection ID is set to 0xFFFFFFFF.

Packet definitions, along with other useful structure definitions are provided in the files PUBLIC_PACKET.LC and PUBLIC_NAME.LC. These files should be included in the custom application's STDAFX.H or otherwise included where used by the application. PUBLIC_NAME.LC has structure definitions which can be used by the custom application to interpret device and device type name files, to associate device name IDs with user-defined alphanumeric device names.
Note that FP_STATUS_LINK packets are used to acknowledge correctly received packets, and if a packet is not so acknowledged, the system may wait for a timeout interval and then retry transmitting the packet. All non-LINK packets received correctly by the third party application should be acknowledged by sending an FP_STATUS_LINK packet to the controller. LINK packets use the FP_STATUS_PKT structure definition, with the sequence number set equal to that in the received packet, data_size set to 1, and data[0] set to the packet_type of the received packet. For the remainder of this document, FP_STATUS_LINK packets will be assumed in all packet conversation examples, and not explicitly shown.
For LINK packets, "correct" means the packet was transported across the physical data link with proper size and with correct CRC value, and does not indicate contextual usage correctness. When desired, contextual correctness is confirmed using FP_STATUS_RESPONSE or FP_STATUS_REPORT packets.
Also note that additional private packet types are used by the system for setup and configuration purposes. Custom and third party applications should ignore all such unrecognized packets.
3) After establishing a socket connection with FSD Router, the custom application should receive an ST_CONNECTION_INFO packet from FSD Router.
From the FSD Router ST_CONNECTION_INFO packet, the custom application should save the router's connection ID for use whenever packets are addressed to the router. The custom application should also use the connection index value from the packet to construct its own connection ID value. The max_packet_size value sent from the Router should be used to limit the maximum packet size sent from the custom application.
The request_reply field in the received ST_CONNECTION_INFO packet indicates whether the originating application expects the sending application to reciprocate by sending an ST_CONNECTION_INFO packet back to the originator. The ST_CONNECTION_INFO packet from FSD Router will always have request_reply set TRUE, and the ST_CONNECTION_INFO response packet send from the custom application to FSD Router should set request_reply to FALSE.
The following code snippet is provided to show how to interpret the ST_CONNECTION_INFO packet received from FSD Router:

```
// process ST_CONNECTION_INFO packet from ROUTER app
switch (((FSD_PKT_HEADER *) m_packet_received)->packet_type)
{
case FP_STATUS_REPORT:
switch (((FP_STATUS_PKT *) m_packet_received)->status_type)
{
case ST_CONNECTION_INFO:
// save the connection ID for FSD Router
m_fsd_router_connection_id =
((FSD_PKT_HEADER *) m_packet_received)->source_id;
// construct the connection ID for the Custom Application
m_custom_application_connection_index =
((ST_CONNECTION_INFO_PKT *) m_packet_received)->connection_index;
m_custom_application_connection_id =
(CUSTOM_APPLICATION_BASE_ID +
m_custom_application_connection_index);
```

4) The custom application should send an ST_CONNECTION_INFO response packet to FSD Router. Again, a code snippet:

```
// send custom application's connection info to FSD Router
send_connection_info_packet (fsd_router_connection_id, FALSE);
VOID send_connection_info_packet (ULONG destination_id, UCHAR reply_state)
{
ST_CONNECTION_INFO_PKT *connection_packet_p;
FSD_PKT_HEADER *packet_header_p;
connection_packet_p = (ST_CONNECTION_INFO_PKT *) packet_buffer;
packet_header_p = (FSD_PKT_HEADER *) packet_buffer;
// set the packet header info
packet_header_p->synch = FP_SYNCH;
packet_header_p->destination_id = destination_id;
packet_header_p->source_id = m_custom_application_connection_id;
packet_header_p->packet_type = FP_STATUS_REPORT;
packet_header_p->packet_size = (USHORT) sizeof (ST_CONNECTION_INFO_PKT);
packet_header_p->sequence_number = // rolling number, 1 - 255, back to 1
```

```
// set the status type value in the packet
connection_packet_p->status_type = ST_CONNECTION_INFO;
connection_packet_p->request_reply = reply_state;
strcpy (connection_packet_p->sw_application_name,
"custom_application");
connection_packet_p->sw_version = 0x0001;
connection_packet_p->hw_type = 0x0000; // Windows PC
connection_packet_p->hw_configuration = 0x0000;
connection_packet_p->hw_version = 0x0000;
connection_packet_p->packet_data_version = PACKET_DATA_VERSION;
connection_packet_p->max_packet_size = MAX_BYTES_IN_PACKET;
connection_packet_p->connection_index = m_custom_application_connection_index;
connection_packet_p->data_size =
(sizeof (ST_CONNECTION_INFO_PKT) - (sizeof (FP_STATUS_PKT) - 1));
// add crc_16
set_packet_crc_16 (packet_buffer, packet_header_p->packet_size);
// send the packet
send_fsd_packet (packet_buffer);
} // end send_connection_info_packet
VOID C_CRC::flash_crc_16_accumulate (USHORT *crc_16_value_p, UCHAR in_byte)
{
#define CRC_CCITT 0x1021
USHORT data;
USHORT index;
USHORT crc_16_value;
/** figure next CRC interim value */
data = (USHORT) (((USHORT) in_byte) << 8);
crc_16_value = *crc_16_value_p;
for (index = 8; index > 0; index--)
{
if ((data ^ crc_16_value) & 0x8000)
{
crc_16_value = (USHORT) ((crc_16_value << 1) ^ CRC_CCITT);
```

```
} else
{
crc_16_value <<= 1;
}
data <<= 1;
}
```

```
*crc_16_value_p = crc_16_value;
} //-* end C_CRC::flash_crc_16_accumulate *-//
VOID C_CRC::set_packet_crc_16 (UCHAR fsd_packet[], USHORT packet_size)
{
/* crc16 of packet */
USHORT packet_index;
USHORT crc_16_value;
// initialize the crc_16 value
crc_16_value = 0xFFFF;
// calculate the crc_16 value for the packet
for (packet_index = 0; packet_index < (packet_size - 2); packet_index++)
{
flash_crc_16_accumulate (&crc_16_value, fsd_packet[packet_index]);
}
// store the crc_16 value in the packet
*((USHORT *) &fsd_packet[packet_index]) = crc_16_value;
} //-* end C_CRC::set_packet_crc_16 *-//
```

5) If FSD Router options are set to NOT require password authentication, proceed to step 7.

If password authentication IS enabled in FSD Router setup options, the custom application will next receive a password request packet:

```
case FP_STATUS_QUERY:
switch (((FP_STATUS_PKT *) m_packet_received)->status_type)
{
case ST_AUTHENTICATE:
switch
(((ST_AUTHENTICATE_PKT *) m_packet_received)->authenticate_type)
{
```

case STD_PW_REQUEST:
6) If the custom application received a password request packet from FSD Router, the custom application must send a valid response packet.
// send a response packet as defined in PUBLIC_PACKET.LC
send_password_info_packet ();
7) The custom application will receive a Password acknowledgement packet from FSD Router. If all is well, the status data value will be STD_PW_OK, and the custom application can proceed with establishing a conversation with the FSD Controller as shown in step 8. Otherwise, additional attempts at password authentication must be made.

```
case FP_STATUS_REPORT:
switch (((FP_STATUS_PKT *) m_packet_received)->status_type)
{
case ST_AUTHENTICATE:
switch (((ST_AUTHENTICATE_PKT *) m_packet_received)->authenticate_type)
{
case STD_PW_OK:
// password is OK, proceed with CONTROLLER conversation
-- OR --
case STD_PW_LOCKOUT:
// bad password, connection dropped by server
case STD_PW_GLOBAL_LOCKOUT:
// bad password received by FSD Router
// from another app, retry password later
```

Custom Application to FSD Controller Conversation:

8) The custom application has now successfully established and authenticated a connection with FSD Router. The custom application can now proceed with establishing a packet conversation with the FSD Controller.
The custom application will send the controller a ST_CONNECTION_INFO packet, using the following controller ID value, with the request_reply field set TRUE so that the controller will reciprocate.

```
#define FSD_CONTROLLER_BASE_ID 0x20020000
```

send_connection_info_packet (FSD_CONTROLLER_BASE_ID, TRUE);
9) The custom application will receive an ST_CONNECTION_INFO packet from the FSD Controller. As above, the custom application should extract the max_packet_size value from the controller's ST_CONNECTION_INFO packet and use it to limit the size of packets sent to the controller.

```
case FP_STATUS_REPORT:
switch (((FP_TEST_TYPE_RESPONSE_PKT *)m_packet_received)->status_type)
{
case ST_CONNECTION_INFO:
```

10) The custom application will receive DEVICE_ELEMENT data packets from the FSD Controller, containing element state data from the devices on the system.

```
case FP_DATA:
switch (((FP_DATA_PKT *) m_packet_received)->data_type)
{
case DT_NAMED_DEVICE_ELEMENT_DATA:
case DT_DEVICE_ELEMENT_DATA:
```

11) The custom application may send DEVICE_ELEMENT data packets to the FSD Controller, containing element state data to control the output states of the devices.

Other Custom Application to/from Controller Conversation:

12) If the custom application is up and running with a valid FSD Router connection prior to the FSD Controller power-up, or after the FSD Controller has been reset, the custom application will receive an STD_SLAVE_RESTARTED report telling the custom application that the controller has been restarted. Whenever an STD_SLAVE_RESTARTED packet is received, the custom application should reestablish a controller connection by sending a new ST_CONNECTION_INFO packet to the FSD Controller as in STEP 8 above.

```
// Received From Controller after power-up or reset:
case FP_STATUS_REPORT:
status_type: ST_SLAVE_STATUS
status_data_type: STD_SLAVE_RESTARTED
```

13) The custom application may send an ST_REPORT_ELEMENT_STATES_PKT to request an immediate report of a device's status data. In a typical application, the initial ST_REPORT_ELEMENT_STATES_PKT packet will have report_after_read set to

FALSE, and de_sequence_number set to 0. If the number_of_device_element_states is set to 1 and the device_name_id, device family, device index, and element index are all set to 0xFFFFFFFF, 0xFF, 0xFFFF, and 0xFF, all enabled element states of all devices present will be reported.
Note that the FSD Controller will not broadcast device-element state packets until an ST_REPORT_ELEMENT_STATES_PKT has been received.
14) The custom application may send an ST_OPERATION_MODE_PKT to set the operation mode of the FSD Controller.
15) If configured, the custom application will receive an ST_NOTIFY_ALARM_TRIGGER_PKT when a configured alarm event has occurred.
16) A note on packet sequence number usage:
For packets issued spontaneously by an application, such as DEVICE_ELEMENT_DATA packets and STATUS_QUERY packets, the application should maintain and use an outgoing packet sequence number. For each packet sent, the sequence number should be incremented in sequence from 1 through 255, returning to 1 as the next value following 255.
STATUS_REPONSE packets must have the sequence number set to the sequence number of the STATUS_QUERY packet to which the response is being sent. Applications compare the response sequence number to the request sequence number to verify the received answer is matched to the appropriate question, maintaining appropriate synchronization between the application and the controller.
17) Miscellaneous notes:
All multi-byte numbers are stored in LITTLE ENDIAN (Intel style) form, with the least significant bytes in the numbers coming first, i.e. at lower addresses, than the most significant bytes.
All packet and structure definitions are in PACKED form, with no pad bytes inserted within the structure (sometimes done automatically by a compiler for data alignment convenience). For the Microsoft VC++ compiler, use the “Zp1” compile option. This is also referred to as “1-byte-alignment” mode.
Time values follow the Microsoft definition of time (__time64_t values), representing seconds past a particular reference time.

Text string values in packets are in ASCII (single byte per char) and should include a 0x00 termination character (C-style strings). The associated data_size value in FP_TEXT_PKT packets includes the 0x00 termination character.
Note that many structures are defined as having a variable size array within the structure. In these cases, arrays are declared with an array size of 1, and are preceded by a number_of_entries variable specifying the actual number of array records present. The actual number of entries may be any value from 0 to a maximum dependent on the data represented. The actual size of the structure, and hence the position of the CRC_16 value at the end of the structure, will thus be dependent on the number of entries present. All packets have a standard header with a valid packet_size value indicating the actual size of the packet structure including any variable length data.
Also note that for structures defined with more than one variable size array, or with nested variable size array, the position of array entries must always be explicitly calculated relative to the position of the first array entry, and the array entries cannot be accessed simply by indexing the array. As a particular example, the FP_NAMED_DEVICE_ELEMENT_DATA_PKT must be linearly "walked through", calculating the device and element data positions for each device in the packet.
A variety of CRC calculation methods are in common use, with sample implementation code freely available from many sources. Not all of these methods produce the same resulting values. To ensure consistent results, use the sample CRC_16 calculation code provided or code that produces equivalent results.

FSD J1708 Controller Specification Sheets

Select the FSD J1708 Controller type below to display its specification sheet.

FSD J1708 Controllers

FSD J1708 Tester – FSD J1708/J1587 system analyzer for monitoring, decoding, logging, testing, and simulating J1708/J1587 packet traffic.

FSD J1708 Bridge – on systems with more than one J1708/J1587 bus, the FSD J1708 Bridge allows access of data from one bus to the other.

FSD J1708 Logger –the capabilities of the FSD J1708 Bridge along with packet logging functions

FSD J1708/J1587 Analyzer and Simulator

FSD J1708/J1587 Protocol Analyzer / Monitor / Logger / Simulator / Test System

FSD J1708/J1587 Tester System for monitoring, decoding, logging, testing, and simulating J1708/J1587 packet traffic. System includes Windows-based software and an intelligent J1708 Tester pod to interface to the J1708 bus.

The J1708 Tester is a full J1708 interface implementation, including packet collision avoidance, detection, and retransmission. The J1708 Tester reports received and transmitted packets, interleaved in the order sent on the bus. The tester also detects and reports packet collisions occurring on the J1708 bus, including broken packets, packets with bad checksums, and otherwise illegal packets.

The user software monitors the J1708 packet stream, shows the transmit and receive packets, and decodes packet MIDs and PIDs to provide a convenient way to analyze the J1708 bus traffic. The packets may be logged to a disk file either as decoded text or in binary form. If saved as binary, can be decoded to an annotated text file.

The system can send J1708/J1587 packets to devices to test their responses. The user can configure customizable predefined packets to send commonly used well-formed J1708/J1587 packets to the J1708 bus. Also, a user can define and send arbitrary packets on the J1708 bus to test device responses to unexpected conditions.

The system can simulate J1708/J1587 packet traffic stream to facilitate long term and stress testing of J1708/J1587 devices and systems. The user can send repeatable test packet sequences to compare known behaviors and recreate observed failure conditions. Packet sequences may be replayed from captured binary log files, from captured or extracted text log files, or from manually-generated packet sequences in text files.

Software customization services are available to provide full decoding of packets for vendor-specific parameter IDs, device specific predefined packet test options, and device specific simulation capabilities.

FSD J1708 Tester, when coupled with an FSD Automation Controller, can become a mixed signal testing system.

Specifications

Inputs:

USB host computer ports

9-12 VAC, 100ma

Outputs:

J1708 interface

Dimensions:

FSD J1708 Bridge Controller

The FSD line of J1708/J1587 monitoring controllers report J1708/J1587 communication packets sent through the J1708/J1587 bus. In situations where more than one J1708/J1587 bus reports data, the FSD J1708 Bridge allows access of data from one J1708/J1587 bus to the other bus. For example, the recommendation for vehicles is for the J1708 system architecture to provide two separate J1708 data buses, one for critical systems, such as engine control, and the other for less critical systems. Engine speed and braking conditions may be logged by a vehicle logic controller unit along with other system states, such as collecting maintenance information, recording driving conditions and recording responses to emergency situations. The FSD J1708 packet bridges allow access to data from one J1708 bus by devices on the other bus.

The FSD J1708 bridge is a highly flexible, standard-product solution for this requirement. The system designer can control the packets mirrored through the bridge by specifying which packet MIDs and PIDs are allowed through the bridge. The bridge unit can be configured to be bi-directional, with independent MIDs and PIDs specified for each direction. Some packet types, such as engine speed data, may occur more frequently than of interest to the other side of the bridge. For this situation, a packet count option can be set for each MID – PID combination so that only one packet per number of packets counted is allowed across the bridge.

The bridge control options are configured using a provided Windows based program, then loaded into FLASH within the bridge.

Specifications

Outputs:

2-J1708 ports

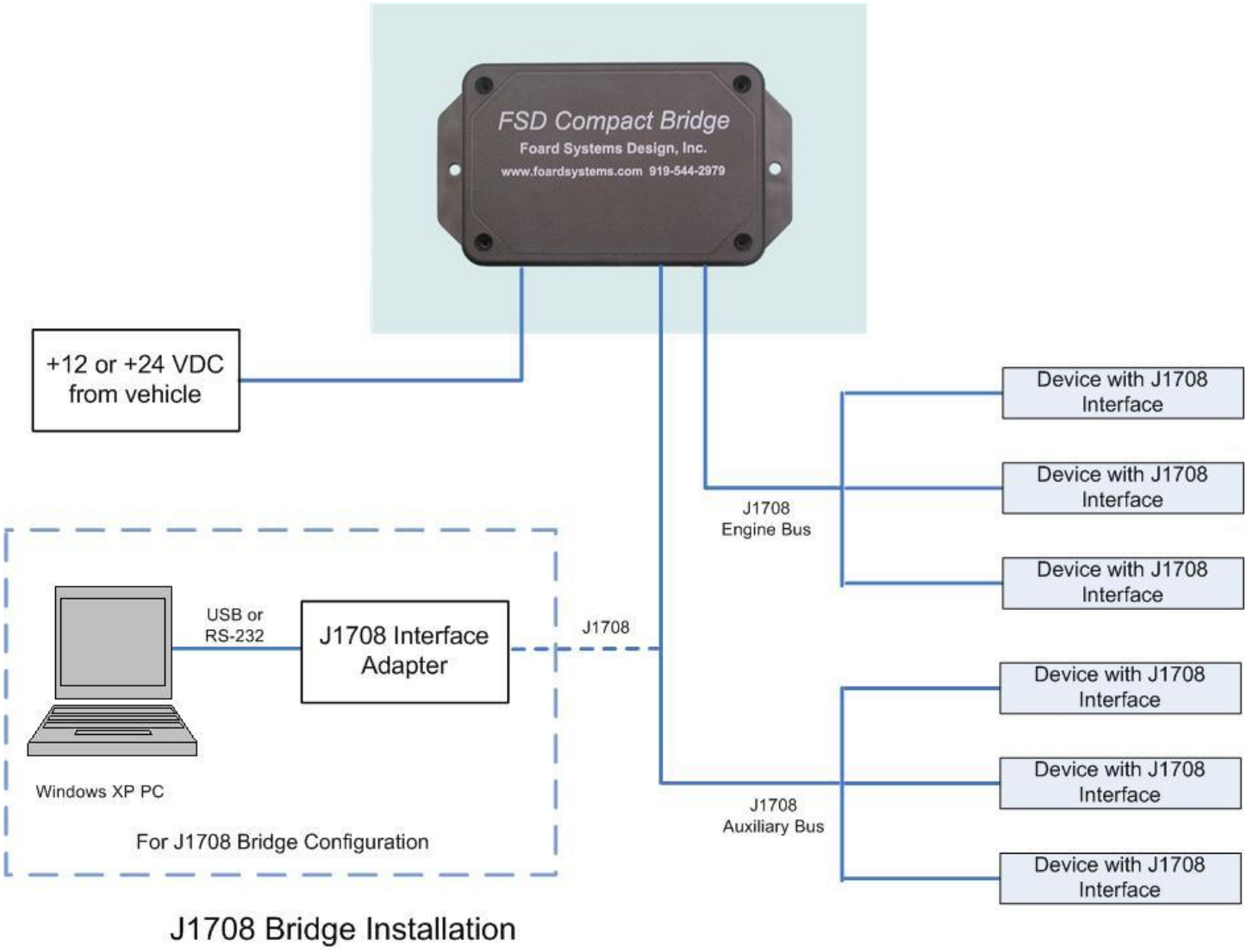
Dimensions:

Controller: 5” x 3” x 1”

Included With Controller:

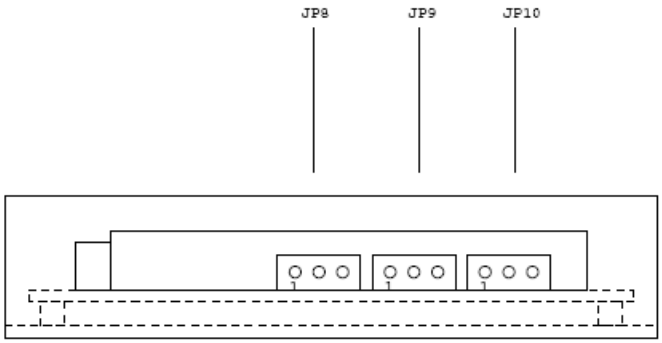
FSD J1708 Bridge

FSD J1708 Bridge Software



J1708 Bridge Installation

J1708 Bridge



JP8 Power Input
1) 24V Input
2) GND Input
3) 12V Input (If 24V not used)

JP9 J1708 Interface
1) SA J1708 +
2) SB J1708 -
3) J1708 GND

JP10 RS232 Interface
1) FSD J1708 Bridge RS232 TXD
2) FSD J1708 Bridge RS232 RXD
3) GND

FSD J1708 Bridge with Logging

FSD J1708 Bridge

The FSD line of J1708/J1587 monitoring controllers report J1708/J1587 communication packets sent through the J1708/J1587 bus. In situations where more than one J1708/J1587 bus reports data, the FSD J1708 Bridge allows access of data from one J1708/J1587 bus to the other bus. For example, the recommendation for vehicles is for the J1708 system architecture to provide two separate J1708 data buses, one for critical systems, such as engine control, and the other for less critical systems.

FSD J1708 Bridge with Packet Logging Option

On-vehicles, the vehicle owner / operator commonly desire data logging features for J1708 systems. Additionally, on-vehicle packet logging is a valuable diagnostic tool for the J1708 system designer. Logging provides a tool to diagnose reported malfunctions. Many malfunctions are difficult to recreate in the laboratory.

FSD provides data logging capabilities as a standard product solution, which can be added to a system without developing custom system software and without impacting the system design. Logging can also be easily retrofitted into an existing J1708 system, or temporarily added for diagnostic purposes.

The J1708 bridge can be equipped with an internal J1708 packet data logging option. Control over logging operation is similar to the control over bridge operation, with packets selected by MID and PID combinations. Packets can be logged from either or both J1708 buses, with separate MID-PID combinations logged from each bus. There is a packet count filter for the logging function. For packet types where the information of interest is presented more frequently than wanted, a packet is recorded one every set number of packet types received. Additionally, a time interval parameter, for each specified MID-PID packet combination, allows logging intervals based on time rather than packet count.

The logging options are configured with the same utility used for bridge configuration. The control data are loaded into the bridge box FLASH. FSD Windows-based software retrieves the stored packet log data from the bridge unit and converts to decoded text form. (The bridge unit's packet offload protocol is available to system designers who wish to dump the log file from the bridge unit directly. For example, automatic wireless transfer to a maintenance facility.)

Specifications

Inputs:

USB host computer port

Outputs:

2-J1708 ports

Dimensions:

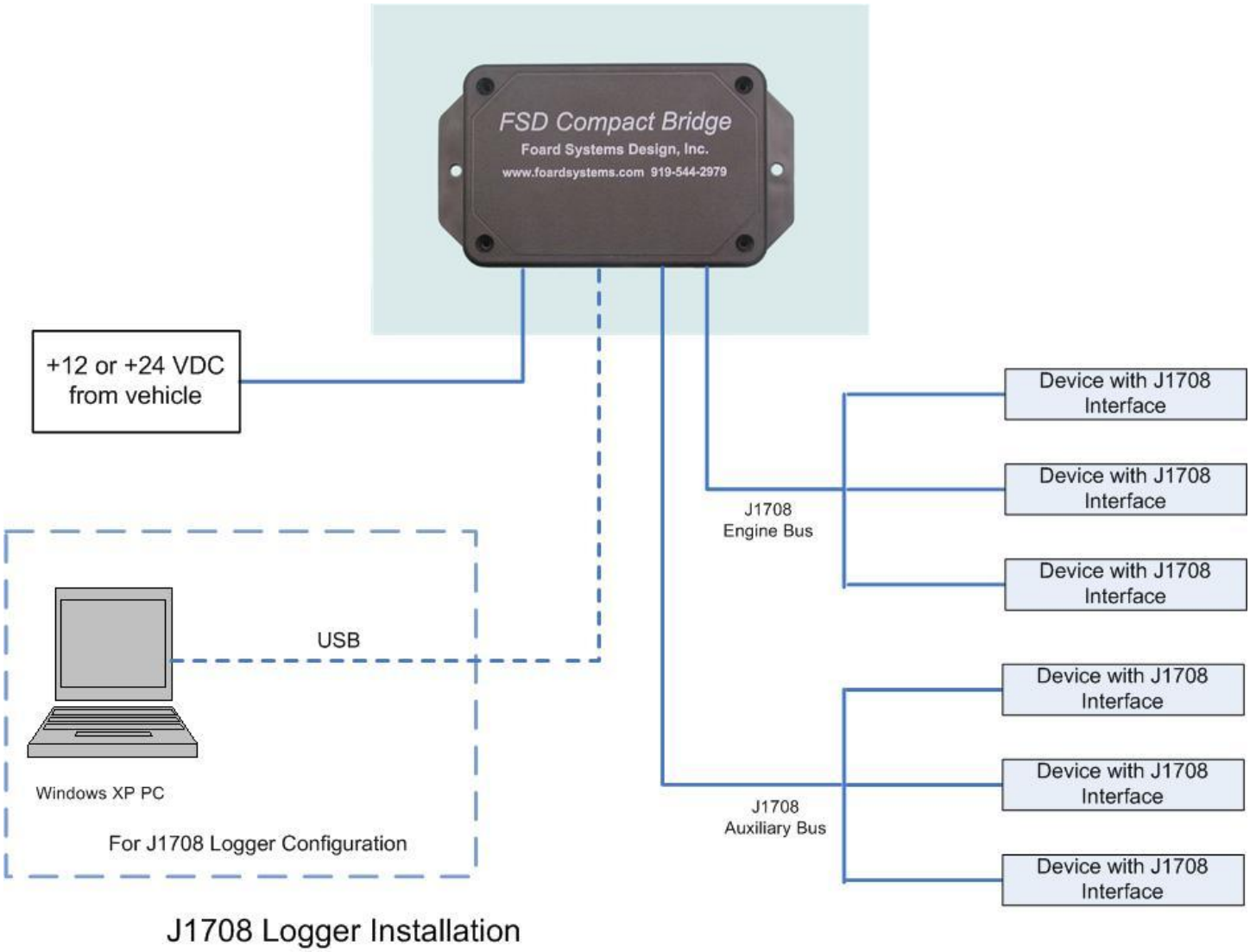
Controller: 5" x 3" x 1"

Included With Controller:

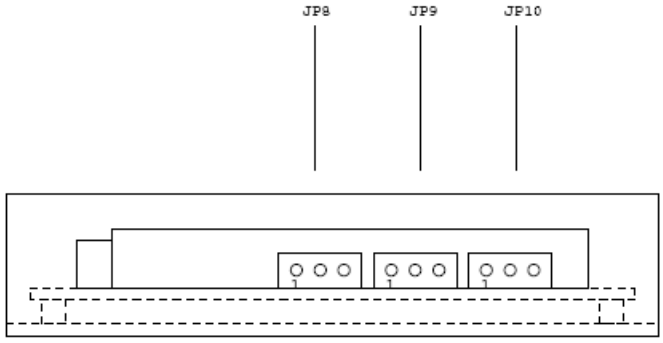
FSD J1708 Bridge

FSD J1708 Bridge Software

Wiring Example



J1708 Logger Installation



JP8 Power Input
1) 24V Input
2) GND Input
3) 12V Input (If 24V not used)

JP9 J1708 Interface
1) SA J1708 +
2) SB J1708 -
3) J1708 GND

JP10 RS232 Interface
1) FSD J1708 Bridge RS232 TXD
2) FSD J1708 Bridge RS232 RXD
3) GND